Granting Privacy and Authentication in Mobile Ad Hoc Networks

Balmahoon Reevana

Submitted in fulfilment of the academic requirements for the degree of Master of Science in Computer Engineering in the School of Engineering, University of KwaZulu-Natal

May 21, 2012

Supervisor: Professor R Peplow

Declaration

As the candidate‟s Supervisor I agree/do not agree to the submission of this thesis

Signed: _____

Date: _____

I ..... declare that

i. The research reported in this dissertation/thesis, except where otherwise indicated, is my original work.
ii. This dissertation/thesis has not been submitted for any degree or examination at any other university.
iii. This dissertation/thesis does not contain other persons‟ data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.
iv. This dissertation/thesis does not contain other persons‟ writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
    a) their words have been re-written but the general information attributed to them has been referenced;
    b) their exact words have been used, their writing has been placed inside quotation marks, and referenced.
v. Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.
vi. This dissertation/thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation/thesis and in the References sections.

Signed: _____

Date: _____

Acknowledgements

To my mother, *Shireena Balmahoon* who has always offered immense moral support and has made my life ever so comfortable, thank you for your guidance and support. To my father, *Vishunduth Balmahoon* who is the pillar of strength for my family, thank you for your encouragement and for always allowing me to exceed my goals.
To my sister, *Tarika Balmahoon*, who is also one of my closest friends, thank you for your everlasting love and support.

Professor Peplow, my supervisor, who went through the tiresome and tedious task of proof reading this dissertation, thank you. The support and guidance you have offered during this research is immeasurable.

Thank you to *Telkom SA Ltd*, for their financial support.

Abstract

The topic of the research is granting privacy and authentication in Mobile Ad Hoc Networks (MANETs) that are under the authority of a certificate authority (CA) that is often not available. Privacy is implemented in the form of an anonymous identity or pseudonym, and ideally has no link to the real identity. Authentication and privacy are conflicting tenets of security as the former ensures a user‟s identity is always known and certified and the latter hides a user‟s identity.

The goal was to determine if it is possible for a node to produce pseudonyms for itself that would carry the authority of the CA while being traceable by the CA, and would be completely anonymous.

The first part of the dissertation places Vehicular Ad Hoc Networks (VANETs) into context, as this is the application of MANETs considered. This is followed by a detailed survey and analysis of the privacy aspects of VANETs. Thereafter, the solution is proposed, documented and analysed. Lastly, the dissertation is concluded and the contributions made are listed.

The solution implements a novel approach for making proxies readily available to vehicles, and does indeed incorporate privacy and authentication in VANETs such that the pseudonyms produced are always authentic and traceable.

Table of Contents

List of Figures

List of Abbreviations

PKI	Public Key Infrastructure
MANET	Mobile Ad Hoc Network
TTP	Trusted Third Party
CA	Certificate Authority
VANET	Vehicular Ad Hoc Network
RSU	Road side Unit
OBU	On Board Unit
ITU	International Telecommunications Union
SIM	Subscriber Identity Module
ROM	Read Only Memory
UDP	User Datagram Protocol
IP	Internet Protocol
CPU	Central Processing Unit
MHz	Mega Hertz
KB	Kilobyte
SSH	Secure Shell
GSM	Global System for Mobile communication
3G	Third Generation of Wireless Technology
TLS	Transport Layer Security

1. Introduction

In recent times, the cost and complexity of wireless communication has dropped dramatically while the usage has risen equally dramatically. During 2002, the number of mobile phone subscribers exceeded the number of fixed line phone subscribers, marking a significant event in the history of wireless communications [**1**]. Bhavnani et al. [**2**] attribute this to the low cost of adding new subscribers to a cellular network. The use of wireless communication has since been increasing. Rao [**3**] has reported that the number of mobile phone subscribers in 2011 was more than 500 million and predicts that 2012 will see an increase in smartphones that surpasses that of laptops. Cisco [**4**] predicts that in 2012 the number of mobile devices will exceed the world‟s population. The growth in mobile devices has made the global workplace become more connected; mobile phones, tablets, Skype and high-bandwidth internet communications allows for more convenient and frequent communication [**5**]. The growth of wireless network devices has given rise to a new field of networking, that of Ad-hoc networks where the fundamental paradigm shift is that these networks have no formal or predefined structure or generally, any central administration or coordination functions which are normally the hallmark of the more historic wired and structured networks [**6**].

Ad-hoc networks may be wired or wireless but the lack of organised structure means that nodes can add to or remove themselves from the network at any time [**6**]. Further, the lack of structure may mean, particularly in wireless networks that two nodes that wish to communicate may be out of signal range of one another and so intermediate nodes may be expected or requested to route the communication packets between the two nodes [**7**].

There are many fields where ad-hoc networks are being applied, some of these being sensor networks, mesh networks and Mobile Ad Hoc Networks [**8**]. Mobile Ad-hoc Networks (MANETs) are composed of mobile nodes that enter and leave groups. A growing field within this class is that of Vehicular Ad-hoc Networks (VANETs) which, as explained by Boukerche [**9**], allow for vehicles to exchange time-critical information that helps improve the safety on roads. The VANET can be used for information transfer between vehicles and much has been written in Plobl [**10**] and others in [**9**] [**11**] [**12**] [**13**] [**14**] [**15**] on the various scenarios where vehicles may obtain value from communication. Messages warning of icy road conditions, accidents, congestion etc., are all potentially extremely useful and could reduce accidents. However, one needs to be sure that the messages are valid and that the network will not be used maliciously. One could for

example conceive of a situation where all traffic is informed of a major accident on a motorway and advised to divert to a different route whereas the sender is merely trying to keep a section of the motorway free so that they can use it as a race track. One method of reducing the likelihood of such malicious use is to ensure that all nodes are registered with some central authority so that nodes caught sending erroneous and malicious messages can be determined and held accountable. According to Aboudagga et al. [**16**] and Sehgal et al. [**17**], this thus means that every node should be registered with some central authority. It also means that nodes must identify themselves as the source of all their messages and anonymous message sources should not be permitted or accepted.

This registration and identification however opens up a different problem in that message senders can now be traced and this lack of privacy may result in many nodes being unwilling to send messages at all. It could also allow other nodes to track the sender for nefarious purposes. Examples from Kargl [**18**] and Weerasinghe et al. [**19**] discuss how a vehicle may be tracked by developing location profiles. Thus it can be seen that there is a need for all messages to be traceable [**20**], so the sender can be held accountable for the messages and yet at the same time, it should not be possible for any node to identify the source of any message or to track a node through multiple messages.

The main network classifications are discussed in section 1.1. This includes descriptions of the applications of wireless networks and Ad Hoc Networks. Section 1.2 discusses MANETS and VANETs in detail. The characteristics, applications and challenges these networks face are elaborated on within the same section. Section 1.2 also provides an introduction to privacy in VANETs. The motivation and objectives for the research are covered in section 1.3. Lastly, section 1.4 describes the outline of the dissertation.

1.1 Networks

Hekmat [**21**] describes networks as a collection of nodes and communication links, where nodes are devices (either fixed or mobile) and are interconnected by communication links, which facilitate communication and allow for the sharing of resources and information among interconnected nodes. There are variations on how these devices are connected to the communication links and what technology the communication links make use of. For example, a fixed line telephone network is a communication network that uses wired connections and makes use of circuit switching (which shares a communication link on a fixed allocation basis) to provide a communication path between two nodes [**22**]. In other

networks, communication between nodes may occur wirelessly, where there is no physical link (for example wire) connecting nodes.

According to Zhu et al. [**23**], wireless communication has grown rapidly within recent decades. It has as a result brought on a new era of mobile applications [**24**]. Choi et al. [**25**] describe the major result of wireless communication as mobility. Mobility supports productivity in a workplace, as users have access to information wherever wireless communication is available and may thus continue working even while moving around [**26**]. According to Gloria and Makoto [**26**] and Hoebekeet et al. [**27**] this mobility creates the opportunity to work while travelling, increasing the worker productivity on business trips. Employees are able to respond to emails while travelling, which increases productivity. Mark and Su [**26**] are of the opinion that some employers feel that freedom from the containment of cubicles leads to increased productivity amongst workers and a better work-personal life balance. This is because employees need not be restricted to a cubicle and may work in some other environment (home, cafeteria, etc.), allowing for a convenient and comfortable work environment.

Perkins [**6**] maintains that the strongest motivator for the increase in wireless communications is the cellular phone. This opinion is shared by Hoebekeet et al. [**27**] and Sun [**28**]. Cellular phones are a standard device that can be used globally. Keshav [**29**], describes a cellular phone as a battery-powered microprocessor with wireless transmitters and receivers capable of performing voice input/output. They are standard devices that require a globally unique, per-user identifier, called the International Mobile Subscriber Identifier [**29**]. This unique identifier is allocated by cellular phone providers and allows them to track and bill for cellular phone usage. Wei [**30**], has listed mobility as one of the factors that have influenced the use of cellular phones. The result of mobility is that communication has become more convenient [**30**]. According to Farely [**31**], cellular phones allow for voice, data and internet access anywhere in the world. Phone calls can be made while moving around (while walking outdoors, for example) thereby making the restriction in terms of movement imposed by fixed line telephones unimportant. Smartphones have made it possible for users to connect to the internet while moving around, allowing for frequent communication via email and fast access to information on the internet. Cellular phones have thus fundamentally changed the way communication takes places and largely contributed to increasing the use of wireless communications [**32**].

Wireless communication has applications in many systems, as described and discussed by Goldsmith [**33**]:

- Mobile Cellular Phones: The author‟s view is that the most successful wireless technology application has been the mobile cellular phone, which provides two-way voice and data communication with regional, national or international coverage.
- WLANs: WLANs support high speed data transmissions within a small region (for example in a building). The wireless devices that access the LAN are typically stationary or moving at slow speeds (a user may be walking in a building while using a hand held wireless device) [**33**].
- Satellite systems: Satellite communication enables voice transmission from remote areas (for example journalists reporting live from a remote war zone). A major amount of power is required to reach the satellites and headsets are therefore typically bulky [**33**].
- Wireless Ad Hoc Networks: These are a collection of wireless mobile nodes that self-configure to form a network without the aid of any established infrastructure. Khayat [**34**] describes the following advantages for wireless Ad Hoc Networks: the cost, maintenance and installation of network infrastructure are avoided.

Based on the literature surveyed, a basic taxonomy of network types has been developed. This is illustrated below and thereafter justified:

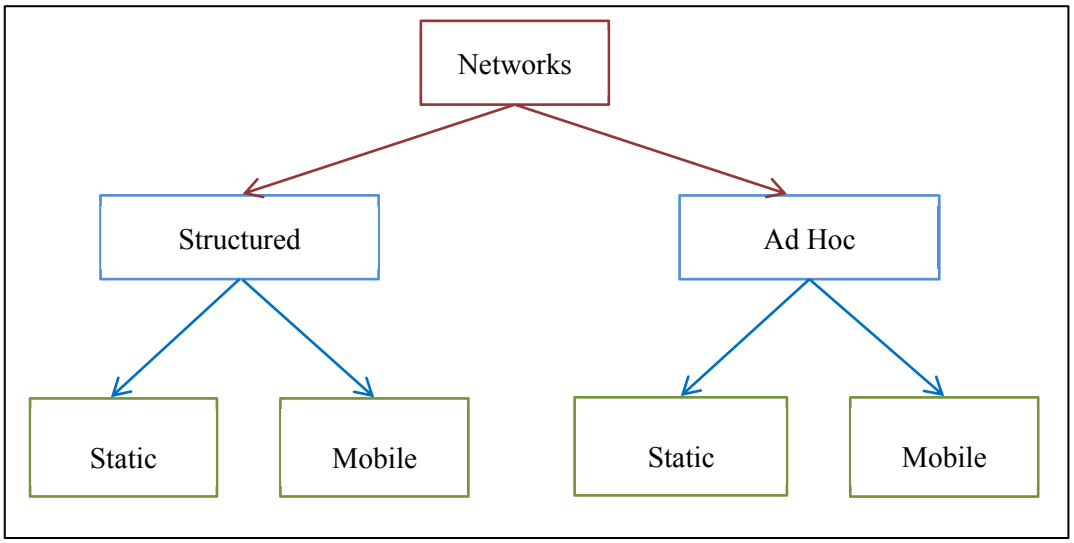

Figure 1-1 - Taxonomy of Networks

The main classifications for networks are structured and Ad Hoc [**35**]. Structured networks contain infrastructure that is made up of routers, switches, gateways etc., which nodes communicate with directly [**27**]. Here, each infrastructure device has a fixed role in the structure. Ad Hoc Networks, on the other hand, have no fixed infrastructure and nodes rely on other nodes in the network to forward messages [**7**]. According to Perkins [**6**], Ad Hoc Networks come together as needed, not necessarily with any assistance from the existing infrastructure. Nodes therefore perform routing functions to cater for the lack of routers and are responsible for forwarding their own and their neighbour‟s traffic. The decision of which nodes forward messages is based on the manner in which the network is connected (and the authority, if any, assigned to nodes), and is therefore decided dynamically [**27**]. According to Chen et al. [**36**], this gives rise to multi-hop routing (many nodes may route a packet before it arrives at the destination).

Structured Networks can either be static or mobile; a fixed line telephone network for example is static and WLANs, UMTS and GSM networks are mobile [**28**]. Structured static networks generally consist of only stationary devices [**21**]. According to Sun [**28**], structured mobile networks have infrastructure support, in which mobile devices communicate with access points connected to the fixed network infrastructure.

Aboudagga et al. maintain that Ad Hoc networks are also either static or mobile [**16**]. Static Ad Hoc Networks are for example sensor networks, where nodes remain stationary and function to sense changes in an environment [**37**]. Sensor networks are often considered Ad Hoc as they connect through each other rather than via central base stations. According to Hoebeke et al. [**27**], Mobile Ad Hoc Networks are networks in which mobile devices form a self-organising and self-administering network.

The difference between the types of structured and ad hoc networks is explained in the following example: When using WiFi in structured mode, there are laptops which all communicate through fixed access points that forward the packets to switches, routers etc. The laptops can either be stationary or mobile. However, when they are used as part of an Ad Hoc Network, they all communicate in a peer to peer method; there is therefore no structure.

Ad Hoc Networks have in recent years attracted much interest [**6**]. The following are some applications of Ad Hoc Networking:

1) Emergency Services

There are instances where internet connectivity is lost due to natural disasters or power outages [**6**]. If authorities responsible for aiding in emergency situations were to cooperate and form an ad hoc network, the response time for emergency situations will most probably decrease. Goldsmith [**33**] is of the opinion that this will enable police squad cars and fire fighting personnel to remain in touch for longer, to provide information more quickly and to respond to an incident faster.

2) Embedded Computing Applications

This refers to intelligent internetworking devices that detect their environment, interact with each other and respond to changing environmental conditions that make human life more convenient.

Weiser [**38**], predicts that there will eventually be a world of ubiquitous computing; in which computers will be all around people, constantly performing mundane tasks to make human lives easier. Ubiquitous computing allows for computing devices to perform their task in such a manner that they are effectively invisible to the user. Perkins [**6**], is of the opinion that once people become used to having simple features on these devices, it seems inevitable that new, smarter embedded applications will be invented.

Perkins [**6**], gives examples of these embedded computing devices as those having access to local information about temperature, light-switch controls, traffic information, or the way toward a water fountain. The information gathered from these devices is used to act intelligently and offer convenience. Traffic information can be provided by devices on roads, which collaborate to determine where traffic build ups or accidents are [**33**].

The evolution of wireless communication presents a new alternative way for mobile communication, allowing mobile devices to form a self-organising and self-administering wireless network, called a Mobile Ad Hoc Network [**27**]. This network type will be discussed in greater detail in the next section.

1.2 Mobile Ad Hoc Networks

Mobile Ad Hoc Networks (MANETs) are groups of mobile nodes that communicate with each other over wireless links [**27**]. The mobile nature of MANETs allows for these nodes to dynamically form into groups. Sun [**28**] defines a MANET as a collection of wireless nodes that can be dynamically set up anywhere and anytime without using any pre-existing network infrastructure. MANETs are a type of Ad Hoc Network and therefore do not rely on any fixed infrastructure to communicate and the routing is performed by nodes, which means that a message can travel from source to destination either directly or through a set of intermediate packet forwarding nodes.

MANETs may be described using the following features (these features have been listed by Sun [**28**]):

- Distributed operation: There is no infrastructure present for the central control of certain network operations (for example security and routing [**28**]), and this effectively implies that the control and management of the network should be distributed among the nodes. Mamatha and Sharma [**39**] state that the nodes involved in a MANET collaborate amongst themselves and each node acts as a relay, to implement network functions.

- Multihop routing: Ad Hoc Network routing algorithms are often multihop [**6**] . The movement of packets from source to destination when nodes are out of direct wireless transmission range occur through one or more intermediate nodes. This rises from the infrastructure-less nature of MANETs.

- Autonomous terminal: Each mobile node is autonomous [**39**], and may function as both a host and a router. This means that aside from the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. Endpoints and switches are therefore indistinguishable in a MANET [**28**].

- Dynamic network topology: Nodes are mobile and hence allow for the network topology to change rapidly [**27**]. The connectivity among the mobile nodes may therefore vary with time. MANETs adapt to the mobility patterns of the mobile nodes, which dynamically establish routing among themselves while moving, thereby forming their own network on the fly [**28**].

- Light-weight nodes: The MANET nodes are generally mobile devices with low CPU processing capability, small memory size, and low power storage [**27**]. These are for example sensor networks, as the sensors are small power constrained devices. These devices therefore require optimized algorithms that implement communication functions. A small battery powered temperature sensor may be power constrained but a car or trucks certainly are not, hence this power consumption constraint varies with the application.

These characteristics allow for MANETs to exist in areas where the use of communication infrastructure is expensive or even where there is not much infrastructure available for communication [**28**]. This is because there is no infrastructure required to implement a MANET. Devices can easily be added to or removed from the network, allowing for MANET applications to be diverse.

Padmadas et al. [**13**] and Sun [**28**] describe military applications as a use of MANETs; networks between soldiers, vehicles, and military information headquarters are maintained using commonplace network technology, which can be easily set up. Military communication is also made easier as MANETs can be set up in remote areas without infrastructure. MANETs become very important for emergency type applications. Some examples of emergency type applications are search and rescue operations, policing and fire fighting and supporting doctors and nurses in hospitals [**27**]. Emergency rescue operations sometimes need to occur where there is damaged communication infrastructure or no infrastructure at all. For example, in a vicinity that a tsunami has recently occurred; the communication infrastructure may be damaged. Since quick establishment of a communication network is needed, MANETs are suitable. Emergency information is relayed to members of a rescue team via small handheld devices [**28**]. MANETs simplify the communication between different network devices. Wired connections, which is seen as tedious [**28**] are replaced with wireless connections.

Even though MANETs have an interesting range of applications, there are various challenges that exist, as mentioned by Padmadas et al. [**13**], and others in [**28**] [**27**] [**39**] [**40**]. These are listed below:

- Mobility-induced route changes [**39**]: The network topology in a MANET is highly dynamic due to the movement of nodes; hence an on-going communication session suffers frequent path breaks [**39**]. This results in frequent route changes.

- Time-varying wireless link characteristics [**13**]: The wireless communication medium is susceptible to many issues: path loss, fading, interference and blockage [**41**]. These cause the transmission range, data rate, and the reliability of the wireless transmission to decrease. The extent to which these factors affect the transmission depends upon the environmental conditions and the mobility of the transmitter and receiver [**39**]. Sun [**28**], lists mobility-induced packet losses and data transmission errors as problems that could also be experienced.

- Routing [**27**]: Due to the fact that the network topology may constantly change, routing packets becomes a challenging task [**28**]. Hoebeke et al [**27**] state that because MANETs are characterised by a multi-hop network topology that can change frequently due to mobility, efficient routing protocols are needed to establish communication paths between nodes. The routing protocols should not cause excessive control traffic overhead or cause an excessive computational burden on the power constrained mobile devices [**27**]. Mamatha and Sharma [**39**], explain that in wireless networks the radio bandwidth is limited and as a result the data rates are lesser than that offered by a wired network. Routing protocols are therefore required to use bandwidth optimally [**41**].

- Security [**28**]: The wireless nature of MANETs makes eavesdropping common [**27**]. This is because messages are broadcast and all nodes in direct transmission range receive messages, allowing for easy interception [**39**]. Hoebeke et al [**27**] maintain that eavesdropping is a passive attack and is usually impossible to detect because it does not produce any new traffic in the network. Active attacks are where malicious nodes are actively involved in disrupting normal operation in the network [**27**]. These attacks are also a risk and active attack examples include deletion, modification, replication and redirection of data packets. Selfish nodes who do not wish to forward packets for other nodes may cause disruption in the MANET as cooperation between nodes to perform network functions (e.g. routing) is necessary [**39**]. Azer [**42**] is of the opinion that the mobile nature of MANETs introduces the following security challenge: the compromise of a legitimate node or the insertion of malicious nodes may go unnoticed in a dynamic environment.

- Power Consumption [**13**]: Sakib [**41**] states that the mobile devices used in MANETs generally have restrictions on the power source in order to maintain portability, size and weight of the device. For most mobile nodes, communication-related functions should be optimised for lean power consumption [**27**], as mobile nodes generally do not have large storage capacities. Conservation of power must therefore be taken into consideration.

These challenges make designing solutions for MANETs difficult. However, the interesting range of uses of MANETs is evidence that it is worth studying this network type further. The security aspect of MANETs is an interesting one. As per any network, security, reliability and availability are three crucial aspects of network security [**28**]. Securing MANETs against malicious attacks is difficult and very often preventative methods are used [**27**]. Before describing some of the preventative methods stated by Hoebeke et al [**27**], a few classical security terms need to be defined (these are merely definitions, which are briefly explained here and covered in greater detail in section 2.1):

- Authentication: proving a user is who they claim to be [**43**]
- Confidentiality: ensuring that information remains secret, and can only be seen by authorized users [**43**]
- Integrity: ensuring that a message has not been modified during transmission [**43**]
- Key-pair: Public-Private key pairs are used in a Public Key Infrastructure (PKI) to encrypt and decrypt messages [**44**]. Encryption is essentially hiding information (related to confidentiality) and decryption is reading information that has been encrypted. The private key is used to sign messages or for decryption. Public keys are used for verifying signatures or for encryption.

The preventative methods for securing MANETs described by Hoebeke et al. [**27**] include authenticating users and ensuring data integrity. Ensuring authentication means that the message source is verified and this leaves little room for impersonation. Integrity ensures a message is untouched, implying it had not been altered after it was sent and therefore no malicious tampering occurred. These are provided for typically by key-based cryptography. In Aboudagga et al. [**16**] the issue of incorporating authenticity in MANETs is raised. It is difficult because it depends on identity verification and there is sometimes no trusted certification authority (CA) to perform the task of confirming identities [**35**]. The CA, above its task of providing an identity to a user, may aid to create trusted relationships by exchanging public-private keys [**28**].

In a network where no CA is present the network has no identity authority; users cannot be authenticated and their identities can therefore not be trusted. There are some methods that have been designed to authenticate users where no CA exists. One example of providing identity authority is given by Zhongwen et al. [**45**] where they present a method for nodes to develop trust through a „certificateless" approach. Here, nodes develop trust from their interactions with other nodes and perform verification on their own. Another approach, which has been used by Capkun et al. [**46**] and Matija [**47**] is that of „self-organization"; nodes produce and distribute their own public keys without the need for an identity authority. There is however no CA to ensure that identities are authenticated. An example of such a MANET with no CA is multiplayer games. It is not of concern if a user is who he/she claims to be and in this case it is acceptable for the network to have no identity authority. This network does not require identity authentication and therefore does not require a CA. The concern surrounding these networks is that since there is no form of identity authority it is very easy for a user to be dishonest about their identity.

There also exist MANETs requiring a CA [**13**], which have some of the following applications: military communications and vehicular services, in which nodes may be located in airplanes, vehicles, or on people. Military users need to know the identity of the person they are communicating with, as confidential information is often transmitted, and as such requires an identity authority. A type of network described by Artimy et al. [**48**] is that where vehicles are nodes and communicate with other vehicles. This is the interesting field of Vehicular Communications. For both these applications, since nodes are mobile and important information may be sent and received, trust and confidentiality are requirements. The CA, being a trusted entity, would ensure that all registered users are authenticated. These networks have proper authentication procedures because a CA is present [**16**]. Here, the node"s identity is known and a CA is the TTP (trusted third party) that assigns an authentic identity to a node. Certificates, which are documents created via cryptographic means and bind a node"s public key to that node"s identity [**49**], are used. Cryptography and certificates are elaborated on in section 2.1.

There are instances where a MANET has a CA present at all times [**50**]. When the CA is always available there is access to an authority that can perform registration and authentication tasks at all times. An example of a MANET with a CA always available is tracking patients in a hospital. A hospital may be entirely wired to pick up patient transmitters and verify their identities. David and Kapidzic [**50**], developed a scheme which caters for authenticating identities while the CA is always available. Secure authentication

is catered for, together with the generation, distribution, storage and verification of certificates. Nodes are required to register with the CA upfront and necessary information is stored at the CA (user‟s details, public key corresponding to user‟s identity, etc.). Certificates are generated and distributed to users by the CA. Since the CA is always available, when certificate verification is required, the certificate is sent to the CA and verified immediately.

In other situations, as described by Padmadas et al. [**13**], access to the CA may be unavailable in some instances. This means that there are applications of MANETs where a CA exists but is not always accessible. The issue of the CA being unavailable has been addressed in many instances using a distributed authority approach. MOCA [**51**], COCA [**52**] URSA [**53**] and DICTATE [**54**] are examples of these approaches. MOCA, proposed by Kravets and Robin [**51**], is a scheme which uses threshold cryptography (decryption can only be performed if the number of entities involved (each holding a shared part of the main private key) exceeds some threshold [**51**]) to distribute the CA functionality over selected nodes. The nodes are chosen amongst themselves based on their physical characteristics and together form a distributed authority. The aim for developing a distributed authority in this case was to minimize the use of scarce resources in mobile nodes. The success ratio ($success\ ratio = \frac{number\ of\ successful\ certificate\ requests}{number\ of\ total\ certificate\ requests}$ [**51**]) is used to analyse MOCA‟s performance. According to the authors of [**51**], MOCA has a success ratio of approximately 90%. Lidong et al. [**52**] proposed COCA, where threshold cryptography is used to sign digital certificates. URSA is similar to COCA, but has a focus on ensuring that misbehaving nodes are not allowed to communicate. URSA has also been analysed in terms of the success ratio; it has a high success ratio of 98% [**53**]. DICTATE, a scheme proposed by Hubaux et al. [**54**], also has a similar structure to COCA, but makes use of a „mother authority‟, which assigns the role of distributed authority node to selected mobile nodes. For each of these methods, there are certain mobile nodes chosen to together perform CA related tasks. These schemes function well for the system they have been designed for; however, there is no record of certificates or their updates for these distributed authority schemes. User identities can therefore not be trusted. Introducing an authority that is responsible for identity management of users will ensure user‟s identities may be trusted.

An example of a MANET application where the CA is present and not always available is a Vehicular Ad Hoc Network (VANET). Artimy et al. [**48**] state that in recent times, many

projects have initiated research to investigate Ad Hoc Networks as a communication technology for vehicle-specific applications, within the wider field of intelligent transportation systems (ITS). According to Padmadas et al. [**55**] ITS are computerised systems that have diverse applications and are connected with Vehicle Transportation. The computerised systems are made up of computers, communications, sensor and control technologies and management strategies [**48**]. These function in an integrated manner to improve the functioning of the transportation systems. They also provide real-time information to increase the safety and efficiency of the ground transportation network [**48**]. Some of the popular applications of ITS are Vehicle Theft Detection and Security Management Systems [**55**]. Vehicle Theft Detection is valuable as a user can be alerted if their vehicle has been stolen and report the theft to the authorities sooner than if the user was not alerted. Security Management Systems allow for vehicles to communicate in an authentic manner and maintain confidentiality and privacy. According to Gunter and Grobman [**14**], many ITS projects make use of short or medium range wireless technology for communication in VANETs.

Harri et al. [**56**] and Papadimitratos et al. [**57**] are of the opinion that VANETs have attracted increasing attention from both research and industry communities within recent years. Sumra et al. [**58**] define the focus of VANETs as fulfilling users‟ requirements on the road and making their journey safe and comfortable. VANETs make it possible to send warnings about environmental hazards (e.g., ice on the pavement), traffic and road conditions (e.g., emergency braking, congestion, or construction sites), and local (e.g., tourist) information to other vehicles [**57**]. Once it is known that there is a traffic jam, road closure or accident ahead, a driver may safely avoid the route. Communication between vehicles is therefore suitable because vehicles are able to distribute warnings to other vehicles. Padmadas et al. [**13**] state that the minimal configuration and quick deployment of VANETs make them suitable for emergency type situations. Messages can also be sent from vehicles to summon for help if needed and to also inform authorities of dangerous behaviour on roads.

There are some special characteristics present in VANETs which are exceptions to general MANETs. These are listed below:

- As per Gunter and Grobmann‟s [**14**] opinion, current standards of wireless technology for wireless Ad Hoc Networks have a limited coverage of a few hundred meters, and this means there may not be allowance for communication

between vehicles in areas where traffic is very sparse. This is however not necessarily the case as advances in wireless communication has been made. For example, direct short range communication (DSRC), which is based on IEEE Standard 802.11a [**59**]. Artimy et al. [**48**] have concluded that DSRC is meant to be used in high speed vehicle environments. DSRC specifies communications that occur over line-of-sight distances of up to 1000 meters between RSU‟s and vehicles [**48**]

- VANETs are potentially large-scale networks [**48**]. There are millions of vehicles on the roads in most countries [**60**]. Since every vehicle needs to be registered with the network, there are a large number of mobile nodes that will be part of the network.

- Road configuration, traffic laws and speed limits on roads affect the mobility of vehicles [**48**]. The vehicle mobility is also affected by the driver‟s driving behaviour and interaction with other drivers. Simulating vehicle traffic is thus a complex task and is a focus of study for applications in transportation engineering [**48**].

- Vehicles are able to provide more resources than general mobile devices used in MANETs. These increased resources consist of large batteries, antennas, and processing power [**48**]. Therefore, conserving these resources in VANETs is not a major concern.

Gunter and Grobmann [**14**] have identified that modern vehicles already provide many helpful features, for example ABS (Anti-Lock Braking System) and ESP (Electronic Stability Program). These systems can however only react when the driver is already in a dangerous situation, hence the goal of providing safety to vehicle occupants should be to rather prevent the driver from even reaching a dangerous situation [**14**].

According to Sumra et al. [**58**], a vehicle is the basic entity module of the vehicular network. VANETs are made up of vehicles (which are equipped with On Board Units (OBUs)) and Road-Side infrastructure Units (RSUs). Calandriello et al. [**61**] state that the OBU‟s may have on-board sensory, processing and wireless communication modules. VANETs allow for vehicles to communicate with one another and with the RSUs. The

RSUs are fixed entities and the vehicles are the moving entities. The following diagram illustrates a high level VANET scenario:

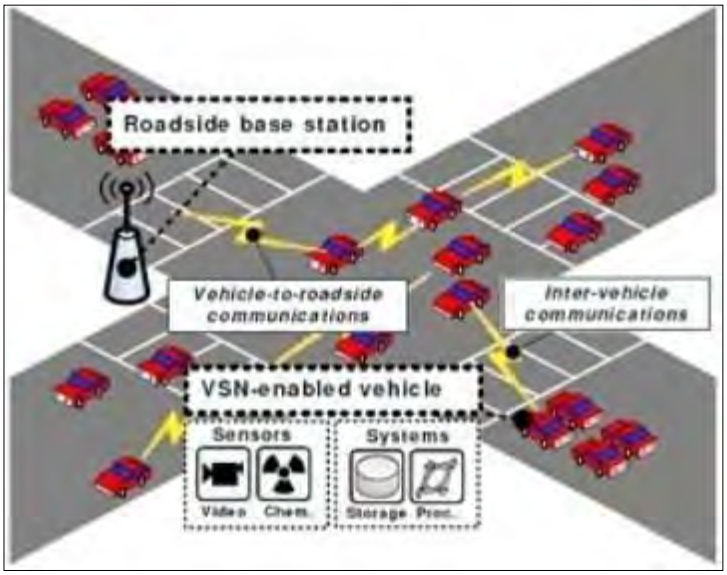

Figure 1-2 – Typical VANET Scenario [62]

Figure 1-2 illustrates vehicles communicating with the RSU (called roadside base station in the diagram) and with other vehicles. The process whereby vehicles communicate with each other is termed Inter-Vehicle Communications and when vehicles communicate with the RSU it is referred to as Vehicle-to-Roadside Communications. A vehicle enabled for VANET services has additional embedded sensors and security modules. This enables vehicles to send warning messages to other vehicles or messages of distress to the RSU/relevant authority.

According to Chen et al. [**36**], the communication in VANETs can either be between vehicles as „one-hop" or vehicles can act as routers, retransmitting messages and communicating in a „multi-hop" method. This means that nodes can communicate directly with another vehicle or can pass messages through a series of vehicles. The type of communication will depend on the nature of the message; for example if vehicles want to communicate individually with another vehicle then „one-hop" communication would be used and if a vehicle wants to contact the CA then a message would be broadcast and passed through the network until the RSU is reached, making the communication „multi-hop". This is made clearer in the architecture view of a VANET presented by Fonseca et al. [**63**], which is pictured below:

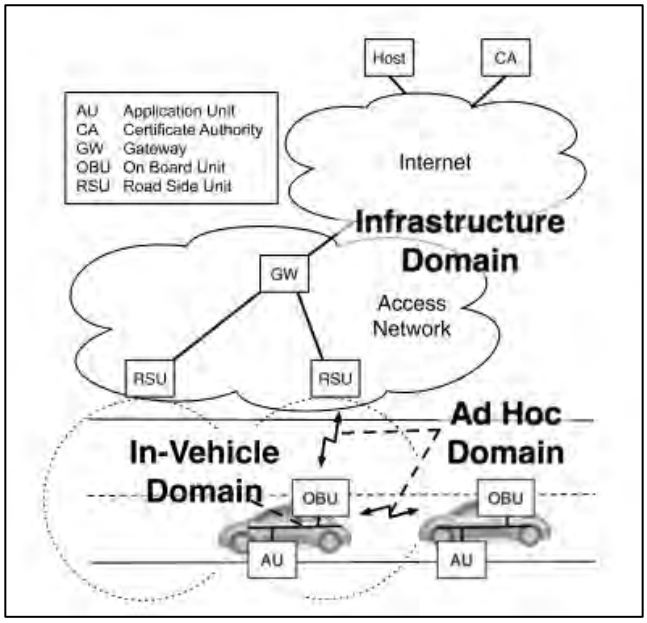

Figure 1-3 - VANET System Architecture [64]

The architecture in a VANET is split into 3 domains; In-Vehicle domain, Ad Hoc Domain and Infrastructure Domain. As can be seen in the diagram above the In-Vehicle Domain consists of an OBU and many AU‟s (Application Units). The AU‟s are user devices for example mobile phones and PDAs that perform certain functions when interacting with the OBU. The Ad Hoc Domain consists of OBU‟s in vehicles and RSU‟s, which are along the roadside. When the OBU‟s and RSU‟s are in range, they communicate wirelessly with each other. The Infrastructure Domain consists of the RSU‟s and the CA. These are connected via the internet and allow for the RSU to act as a proxy to the CA. This domain also provides connectivity to internet services [**64**]. Access to the infrastructure for OBUs is provided by the RSU. Multi-hop communication is used between OBU‟s and RSU‟s when packets are forwarded from one OBU to another to reach the RSU [**57**].

Papadrimitratos et al. [**65**] maintain that VANETs are developed as a means to enhance transportation safety and efficiency. Cooperative collision avoiding [**15**] is one such example. The high speed of wireless communication allows drivers to receive alerts in advance, so when there is a sudden stop/accident ahead, a driver has enough time to stop the vehicle before an accident occurs. This contributes to providing safer transportation. Safety applications are just one of the applications for VANETs, and are discussed below, together with other applications:

1) Safety Applications

VANETs are able to significantly reduce the delay in propagating emergency warnings [**48**]. The vehicles exchange messages to inform each other about events and dangers on the road. A vehicle is able to recognise a dangerous situation and can instantly warn neighbouring vehicles. This allows for a faster reaction to the situation. The information for these warning messages comes from the information derived from sensors in the vehicle: ABS, ESP, etc. Information about traffic congestion can also be sent. According to Emmelmann et al. [**11**], an example of a warning message that the vehicles can send is Emergency Electronic Brake Lights. This allows for sudden braking of vehicles in the forward path to be highlighted as a hazard, asking vehicles to slow down and helping to prevent multi vehicle pile-ups and other accidents.

The on-board sensors may also detect events such as the deployment of airbags (as a result of a collision), loss of tyre traction or sudden application of brakes [**58**]. Safety-related applications include proximity warning, road obstacle warning, and intersection collision warning [**48**]. The objective of these safety applications is to use Vehicular Communication to collect surrounding vehicle dynamics and warn the driver when a collision is likely [**48**].

The alarm signals from emergency vehicles (police cars, fire engines, ambulances, etc.) could also be sent as a warning [**10**]. The emergency vehicle can send its current position, time and destination or desired route and other vehicles can stay clear. The reaction time to the scene of an accident for these emergency vehicles is thus decreased. The addition where infrastructure behaviour can be influenced by the signal given by the emergency vehicle (for example, traffic lights remaining green when the emergency vehicle approaches [**10**]) is also viable to decrease an emergency vehicle‟s response time.

2) Automated Highways [**48**]

These include the automation of certain driving functions in order to increase driving safety and improve the capacity of highways [**48**]. Blum et al. [**66**] provide the following examples for automated highways: assisted/automated over-taking and lane merge, automatic cruise control and emergency vehicles announcement are some of these driving functions that could be automated. Using Vehicle-to-

Roadside Communication, applications such as hidden driveway warning, electronic road signs, intersection collision warning, and railroad crossing warning can also be included [**48**]. These allow for safe driving, as drivers are assisted and warned when necessary while driving.

3) Local Traffic Information Systems

According to Padmadas et al. [**55**], traffic information may be distributed from the RSU to vehicles via radio broadcast or on demand via mobile cellular phones. RDS (Radio Data System) is a technology which embeds certain information into FM (Frequency Modulation) radio broadcasts [**67**]. It is currently implemented in Europe and the United States to broadcast local traffic information [**67**]. While the radio is activated to receive these broadcasts, traffic updates for the local vicinity are provided.

A suggestion to distribute traffic information differently is by using on-board sensors, GPS and digital maps to develop a powerful traffic information system [**48**]. Through VANET communication, the traffic information may then be rapidly and cheaply distributed [**48**]. Traffic information regarding the driver"s current area or an area they are going to enter is of concern to drivers. The level of abstraction of traffic information thus needs to increase as the distance from the source increases.

4) IP Based Applications

Nowey and Plobl [**10**] describe the use of these applications for passenger comfort and entertainment. The traditional IP-based services (e.g., email, web access) are used to access applications and they thus require connectivity to the Internet [**48**]. Some examples of these applications that are given by Artimey at al. [**48**] are online games and promotional broadcasts from companies trying to sell a product. This however contradicts the characteristics of a VANET, as there is often no central access. The vehicle therefore may at times not be connected to the internet. These applications could also potentially compromise safety as it may reduce concentration and distract drivers.

These VANET applications make for more safe and convenient driving. Being able to summon an ambulance automatically in the event of an attack or notify the police if a

vehicle is being hijacked will aid in improving safety on roads. Further, communicating with other vehicles allows for convenient information exchange regarding warnings on the roads.

The distinct characteristics of VANETs which give rise to many applications will however create complications during deployment [**66**]. Some of these challenges are listed below:

- High Mobility

  Sakib [**41**] highlights the fact that since vehicles move a lot, and might opt for broadcast communications, and protocols cannot be handshake based. Vehicles therefore need to be able to authenticate themselves without many exchanges of information. If many interactions are required for authentication between vehicles then due to the high mobility, vehicles may be out of range of each other before finishing the authentication procedure. The high mobility also creates problems in terms of short-lived paths between nodes which cause network partitioning [**66**]. Su et al. [**68**] state that routing protocols that attempt to manage short-lived paths are flow-oriented, and make use of node mobility information to predict the stability of routes in a source-driven protocol.

- Real time delivery of messages

  VANETs have time constraints in the safety applications mentioned above because they are used in emergencies for informing other vehicles and the CA of collisions, accidents and hazards [**41**]. There are therefore strict deadlines that must be met; else the effects could be major. If an accident has just occurred, emergency personnel should be deployed to the scene immediately. Delays could result in a seriously injured person dying or major traffic congestion occurring due to the accident. The high mobility also means that vehicles will not have contact with other vehicles for a long time [**11**], and establishing a secure channel must therefore not take long; this further implies the importance of real time delivery of messages. Schaub et al. [**69**] states that usage of the available communication time should be maximized, which means that bandwidth needs to be used efficiently and the communication overhead should be low.

- Location Awareness

  Since certain location based services require the use of a GPS or other specific location based instruments, any error in these devices is likely to affect the

VANET application [**41**]. This means that these devices need to be installed correctly, maintained regularly and the responsible party should be informed immediately if devices malfunction.

- Security

  VANETs do not have a structured network and may have to allow untrustworthy nodes to route control and data messages [**66**]; securing the VANET is thus very difficult. Due to the fact that potentially untrustworthy nodes route messages, the messages are subjected to corruption. Providing secure routing, secure transport protocols and malicious user detection is important for maintaining security [**66**]. Samara et al. [**70**] maintain that VANET security should satisfy four goals; message and source authenticity, message integrity, privacy (the node sending the message cannot be identified and tracked) and system robustness. Message authenticity implies that the message is from who it claims to be from, whereas source authenticity is needed to ensure that the sender is who they claim to be [**65**].

Solutions need to be developed to address these challenges, which will ensure that VANETs are implemented successfully and securely. According to Ma et al. [**24**] and Artimy et al. [**48**], wireless communication has been proposed to allow for nodes to communicate fast and also allow for communicating irregularities to an authority within good time.

Papadrimitratos et al. [**57**] have described the distinct features of Vehicular Communication as a double edged sword. This is because even though these features and the interesting applications of VANETs are valuable, there are a significant set of abuses and attacks that become possible. For example, if an attacker “contaminates” large portions of the vehicular network with false information. A compromised vehicle may then transmit false warnings, which will be read by all vehicles in the area. These false warnings can give rise to unnecessary route changes and accidents. This is listed as a problem in two of Papadrimitratos et al.‟s writings [**57**] [**65**]. Fuentes et al. [**71**] highlights the concern that a vehicle may also forge messages and pretend to be another entity, for example an emergency vehicle, thereby misleading other vehicles to slow down and yield. This could cause accidents if vehicles brake too fast or move out of the way for these masquerading emergency vehicles. Another type of attack could be where a malicious user attempts to track vehicles [**57**]. This is achieved by using many receivers and recording messages transmitted by vehicles (safety beacons that report a vehicle‟s location are especially suited

[**57**]). Personal information about users may also be compromised during this process, thereby compromising the user‟s privacy [**65**] [**71**]. Chaurasia et al. [**72**] are of the opinion that in order to prevent these types of attacks, security and privacy-enhancing mechanisms are necessary. The need for privacy-enhancing mechanisms is also highlighted in Papadrimitratos et al. [**57**] and others in [**65**] [**73**]. Gerlach [**74**] explains that if the vehicle‟s permanent identity is not masked (i.e. privacy is not implemented) it would be possible for malicious nodes analyzing packets in a certain area to create detailed location profiles of vehicles. This problem is also highlighted as a concern by Weerasinghe et al. [**19**] and others in [**69**] [**75**]. This breaches the driver‟s privacy as there is a strong correlation between vehicle and driver; most vehicles have very few drivers [**72**]. The concern is what messages the vehicle sends and at what time over several days, weeks or even months. This is because there will be possibilities of establishing patterns at certain locations over long periods of time. It can result in a driver‟s personal daily driving patterns and possibly personal data being disclosed [**19**]. Integrity is another important issue in VANETs as altering the contents of messages would create problems for users [**58**]. Without these mechanisms, VANETs could make anti-social and criminal behaviour easier [**57**].

Kargl et al. [**76**] maintain that privacy is an important attribute when designing Vehicular Communication Systems because it is a basic right and many developed countries have implemented it as law. The authors are of the opinion that new technologies should be designed such that it is possible to retain this right. If the vehicle‟s identity is known, there is a high likelihood that the driver is known [**72**]. The vehicle, and therefore the user, could easily be targeted for an attack or theft. It is also not desirable for a user‟s daily routine to be tracked and hiding the user‟s identity will prevent tracking. The vehicle‟s identity must therefore be anonymous. Privacy is also necessary in VANETs for further reasons, which are covered later in Chapter 2.

Even though privacy is necessary, it becomes a problem when the vehicle is entirely anonymous. This is because liability attribution is required by the legal authority in the event that malicious use (for example traffic offence or false warnings) has been detected [**73**]. The authority needs to be able to trace the vehicle so it can be revoked/fined if need be, thus traceability of the vehicle is a requirement. Tracing the vehicle will not be possible if the vehicle is entirely anonymous as the authority would not know the permanent identity of the vehicle. It is therefore necessary to allow for the authority to trace the vehicle while the permanent identity is not disclosed to other vehicles. These security requirements of

authentication, privacy and traceability allow for secure identification and communication while also maintaining a trustworthy system. “Trustworthy” is defined by Sumra et al. [**58**] as a system or components of a system (vehicles and infrastructure) that behave in an expected manner. This definition can be considered a problem when a hijacker for example behaves in an expected manner, as the hijacker cannot be trusted. The expected behaviour therefore needs to be with innocent/righteous intention. There is ideally no malicious or selfish behaviour as this is not what is expected. A CA is necessary to promote trusted identity authentication [**58**] and this is performed by the CA in most instances (elaborated on in sections 2.2.2 and 2.2.3)

Authentication allows for the source of a message to be confirmed. Vehicles need to register with a CA in order to have their identity assigned, which may be verified at a later time. According to Hubaux et al. [**12**], a type of an existing traditional government based vehicle registration system is one where every vehicle is required to be registered with its national or regional authority. Fuentes et al. [**71**] state that manufacturers assign each vehicle a Vehicle Identification Number (VIN) and legal authorities require vehicles to have a license plate; both contribute to uniquely identifying the vehicle. Upon registration with the authority, a unique identifier (license plate) is assigned to the vehicle. In parts of the United States of America and European Union, there has already been significant progress toward registration authorities identifying vehicles though their license plates [**12**]. This is achieved using image processing techniques to identify license plates and thereafter linking the license plate to the registered user. A method which does not incorporate physical license plates, and uses a method termed „Electronic license plates“ is that discussed by Hubaux et al. [**12**]. The electronic license plate is described as a certified identity that a vehicle provides to an authority via a wireless link. Here, authorities ensure each vehicle has a public-private key pair and a certificate (binding its identity to the public key) [**71**]. This caters for identity management of the vehicle, as it is authenticated by its certificate. According to Chim et al. [**20**] the certificate is important in order to cater for authentication and traceability. This electronic process of authenticating vehicles however allows for the vehicle‟s identity to be known, thereby allowing the vehicle to be tracked. This is because the single public-private key pair and certificate always remain the same.

Malicious users tracking vehicles is a problem that arises due to the need for authenticity. Authenticity requires that an identity is assigned to a vehicle in order to verify the source of a message and to hold the vehicle accountable for any malicious use. The vehicle‟s identity however does not change, as it is the identifying attribute for the vehicle. This

allows for vehicles to be tracked, as messages sent by the same vehicle can be linked [**65**]. In order to prevent tracking the vehicle‟s identity needs to be concealed; privacy is thus necessary [**57**]. The need to uniquely identify the vehicle however hinders privacy because it allows for the vehicle to be traced [**72**]. It can easily be seen that requirements of authentication and privacy are conflicting. Fuentes et al. [**71**] state that it is necessary to design a mechanism that balances privacy and authentication. This is supported by Samara et al. [**70**].

The research is centered on the privacy aspect in VANETs. Providing privacy and authentication is a major concern, and has been addressed in the research. The motivation and objectives for the research are presented next, followed by the dissertation outline.

1.3 Motivation and Objectives

According to Sun [**28**], networks generally have a security requirement of authentication. This is because proving a user is authentic proves they are registered with the network and they are who they claim to be. Their identity can therefore be trusted. It implies that through authentication, trust breakdown or abuse can be traced back to the source and the source can be held accountable. As already mentioned, a widely used method for authentication is certification, which makes use of a certificate to verify the identity of a vehicle. Certification and use of a permanent attribute (which is a unique attribute that can be used to identify a user) can therefore aid to grant authentication and traceability.

As mentioned before, Kargl et al. [**76**] state that privacy is a basic right and should therefore be granted to users. Fuentes et al. [**71**], describe forgery, masquerading and tracking attacks that may occur in VANETs if privacy is not granted. In the event of forgery or masquerading, incorrect messages may be sent and innocent vehicles could be revoked by an authority. Tracking attacks may result in vehicle occupants being attacked. Further, in VANETs, knowing the source of a message implies that the vehicle is known [**77**]. To counteract this, the vehicle‟s identity must be unknown. A method to ensure that the vehicle‟s identity is unknown is to hide the vehicle‟s correspondence and identity. This is the aim of privacy according to Papadrimitratos et al. [**65**] and Chaurasia et al. [**72**]. Privacy thus prevents a user from being monitored, followed or traced. Both authentication and privacy are necessary in VANETs, as ensuring the CA can trace the vehicle when needed and hiding the vehicle‟s identity are important. A mechanism that incorporates both is therefore required.

It has been pointed out by Calandriello et al. [**61**] that a challenge with VANETs, which affects authentication, is that the CA may be unavailable at times. In a VANET, driving predominantly in a high density urban environment makes it possible to always have access to a CA. While travelling between urban centres, it is likely that there are short periods of no access to the CA. This may only be for a few kilometres and hence the periods without CA access will generally be rare and brief. However, for vehicles travelling mainly around rural areas and small villages there may be weeks without access to a CA. This means that the CA may be unavailable for authentication at times. The system should however be able to cope with providing authentication and privacy in scenarios with limited CA access.

This research provides a solution for the conflicting tenets of security, authentication and privacy, in a VANET. Authentication is determining that the message is from who it claims to be from [**71**], and privacy is masking the real identity of a user [**65**]. Since these tenets make provision for opposite goals, they conflict one another. There are many reasons for implementing privacy and authentication in VANETs which have been explained above while making reference to [**57**] [**65**] [**72**] [**73**] [**58**] [**12**] [**71**] [**70**]. Lawson [**78**] states that privacy is often implemented via the use of a false identity (or pseudonym). This is explained in greater detail in Chapter 2. The focus of this research is to design a pseudonym generation mechanism that will allow a vehicle to create a trusted certificate based on a generated pseudonym, in the absence of the CA. Since the CA is responsible for authentication management in the network it should be able to trace the owner of the pseudonym. To ensure that privacy is maintained other nodes must not be able to trace a pseudonym to a user or to link two or more messages coming from a particular user.

1.4 Dissertation Outline

The dissertation is organised as follows:

Chapter 1 covers a broad view of networks and hones in on VANETs. Section 1.1 discusses the taxonomy of networks and differentiates between structured and Ad Hoc Networks. Section 1.2 presents the mobile type of Ad Hoc Networks (MANETs); its structure, applications and challenges are thereafter discussed. VANETs are introduced as an application of MANETs and are thereafter explained in terms of their structure, communication methods, applications and challenges. The security threats in VANETs and the need for privacy and authentication is highlighted. Section 1.3 states the motivation and

objectives for the research and section 1.4 outlines the structure of the dissertation. The chapter is concluded in section 1.5.

Chapter 2 focuses on describing privacy in VANETs. Pseudonyms and their use are explained initially. The need for privacy in VANETs is also explained. Possible attacks on the privacy of a VANET are mentioned and some solutions presented. Section 2.1 describes certification and introduces the concept of certified pseudonyms. The four main pseudonym generation methods are discussed in detail in section 2.2. Their shortcomings and variations are also described. This is followed by section 2.3, which describes three methods in which pseudonyms can be re used. The conclusion in section 2.4 brings the chapter to an end.

Chapter 3 presents and analyses the solution to the proposed method. The requirements of the system are initially presented followed by a detailed description of the solution development. In section 3.1, a proxy certificate which provides authentication, privacy and traceability is developed. Thereafter in section 3.2, transactions that indicate the protocol operation is presented. Section 3.3 ends the chapter; this section contains an analysis of the solution in terms of a discussion and ways in which the solution copes for certain attacks.

Chapter 4 is the final chapter of the dissertation. The research is summarised and the solution is concluded. The contributions made during the research are thereafter indicated.

1.5 Conclusion

Networks have been divided into two main groups; Structured and Ad Hoc [**28**]. The characterising difference is that Ad Hoc Networks do not have any fixed access points. Ad Hoc Networks therefore need to compensate for network functions (for example routing), that are normally provided by infrastructure, through the use of network nodes [**6**]. These networks do not take much time or expense to set up, and are therefore suitable for an interesting range of applications, mentioned by Goldsmith [**33**]. MANETs are the mobile version of Ad Hoc Networks and have many advantages due to the mobility of nodes. They may be used in many applications, for example: military applications, emergency services, commercial applications and entertainment applications [**27**]. The mobile devices are however subjected to challenges in certain applications. This is because they have constrained power resources due to their small size and experience routing issues due to the mobility of nodes. Vehicles on the other hand, do not pose this difficulty.

A VANET is an application of MANETs in which vehicles are nodes and communicate with each other and an authority. VANETs are suitable for implementing many applications: Safety, Automated Highways, Local Traffic Information Systems and IP Based Applications [**48**]. These applications aim to make roads safer and allow for convenient driving. VANETs are highly mobile and require messages to be delivered in real time. These requirements create difficulties when designing solutions for VANET systems. One of the challenges is securing the VANET. Forgery, masquerading and tracking are issues that arise and vehicles thus require both privacy and authentication [**71**]. Privacy is not effective without authentication because the vehicle‟s real identity is required by authorities when the user has performed malicious acts [**70**]. The vehicle also needs to be traced by the authority in such an instance. Privacy, authentication and traceability are thus major concerns in VANETs.

The motivation for the research and objectives were presented. The objective is to develop a mechanism which allows a node to produce authentic pseudonyms for itself while being traceable by the CA. The vehicle‟s privacy must be maintained throughout the procedure. The dissertation outline described the structure of the dissertation. The privacy aspect of VANETs is discussed in the next chapter, followed by a chapter which details the proposed solution.

2. Privacy in Vehicular Ad Hoc Networks

As mentioned in the previous chapter, privacy is a major concern in VANETs. Privacy is a broad field that includes many different aspects and has been categorized into the following separate but related concepts by Kargl [**18**]:

- Information privacy: This involves the establishment of rules governing the collection and handling of personal data such as credit information and medical and government records. It is also known as data protection
- Bodily privacy: This concerns the protection of people‟s physical selves against invasive procedures; for example genetic tests, drug testing and cavity searches
- Privacy of communications: This covers the security and privacy of mail, telephones, e-mail and other forms of communication
- Territorial privacy: This is concerned with setting limits on intrusion into the domestic and other environments such as the workplace or public space; for example searches, video surveillance and ID checks.

In VANETs, the privacy concern surrounds information privacy and communication privacy [**18**]. VANETs potentially allow for disclosure of vehicle location information [**75**]; a malicious node eavesdropping on all traffic in an area is able to reconstruct long traces of the whereabouts of majority of vehicles within the same area [**19**]. Kargl et al. [**75**] and Gerlach [**74**] maintain that this problem is addressed by providing privacy enhancing mechanisms. Privacy allows for a vehicle to communicate with other vehicles without disclosing its permanent identity [**72**] [**79**]. This is achieved by hiding the vehicle‟s permanent identity so that it is not visible to other vehicles. Fonseca et al. [**64**] make use of a false name (pseudonym) to mask a vehicle‟s permanent identity, thereby providing privacy. Privacy schemes used by Heesook et al [**7**], Chauraisa et al. [**72**] and Calandriello et al. [**61**], also employ pseudonyms for privacy.

This chapter discusses how privacy is catered for through the use of pseudonyms and thereafter describes the need for privacy in VANETs. Certain attacks on the privacy aspect of VANETs are then presented. This is followed by a section on certification. Thereafter, the chapter focuses on the important issues of how pseudonyms can be generated and re-used. There are four methods of pseudonym generation that have been found in the literature and these are discussed in sections 2.2.1 – 2.2.4. Methods in which pseudonyms are reused play a major role in determining how well the system meets privacy

requirements and this is covered in section 2.3. The main pseudonym reuse methods surveyed are presented in sections 2.3.1 – 2.3.3.

According to Beard [**80**], the word pseudonym is derived from two Greek words; *pseud* (meaning „false“) and *onyma* (meaning „name“). Pseudonyms are therefore false names and are used to hide the user‟s permanent or true identity, which in effect preserves privacy [**78**]. Chaurisa et al. [**81**] state that the function of the pseudonym is to obtain and sustain anonymity. It allows for a vehicle to interact with other vehicles anonymously. Pseudonyms are ephemeral and distinct pseudonyms hide their relation to each other and to the user's identity [**81**]. Pseudonyms make it difficult to determine the real identity of the user, hence the source of a message cannot be determined. In terms of VANETs, using a pseudonym for a vehicle means that the vehicle a message originated from cannot be traced. The purpose of pseudonyms is so that the vehicle‟s identity would be different for each conversation and it would not be possible to determine what identity the same vehicle will have at a later time.

Nodes should ideally be allowed to keep their correspondence private so that confidential information is not leaked to the rest of the network. Mahajan and Jindal [**82**] indicate this using the scenario where a vehicle wants to access certain services from a RSU; the vehicle does not want other vehicles to know who they are or what they are doing and therefore needs to maintain privacy during its communications. The same sentiments are shared by Fonseca et al. [**64**] who further state that the driver‟s privacy should be respected.

If privacy is not implemented, problems may arise if a vehicle is targeted for an attack. A vehicle whose permanent identity is known could be travelling with a low fuel reserve and request for help, but because the vehicle‟s identity is known an attacker monitoring communication in the network will be aware that there is a vulnerable vehicle on a road and could follow the vehicle until it has run out of fuel and possibly attack the occupants and steal all valuable items in their possession. The vehicle occupants could then be stranded without a means of contacting the authorities. However, if the vehicle‟s permanent identity is hidden from all other vehicles and can only be seen by the authorities then only authorized personnel will know which vehicle has requested help and would be able to assist accordingly. Therefore, for the safety of vehicle occupants it is necessary that the permanent vehicle identity is kept secret from other vehicles and known only to the relevant authority. It is also necessary to protect the vehicle owner‟s belongings. For example, if an attacker finds out that every Tuesday morning at 07:30 a particular car is

always at an intersection a large distance from its home, this could be an appropriate time to rob the home. In order to reduce the opportunity to link pseudonyms, Lu et al. [**83**] and Eckhoff et al. [**84**] propose changing pseudonyms in *mix zones*. This is a pseudonym reuse method, which is discussed in section 2.3.2.

According to Hang et al. [**85**], the main attacks on privacy in VANETs are linking pseudonyms and malware. Linking pseudonyms, which is also mentioned as an attack on privacy by Gerlach [**74**], is a passive attack where the network traffic is captured and analysed; persistent malicious nodes attempt to link the previous pseudonyms to the current ones. Pseudonym attributes (e.g. speed) are used to provide the link. This linking is explained in section 2.3.1 and 2.3.2. Linking pseudonyms is possible in a situation where it is possible to determine that two pseudonyms have come from the same vehicle and [**85**] proposes using *mix zones* as a solution; this is discussed in section 2.3.2. Hang et al. [**85**] describe malware attacks as software attacks. Mell et al. [**86**] explain that malware attacks include manipulating messages, crashing or hacking on board units (OBUs), and using a program to compromise the confidentiality, integrity or availability of the victim‟s data. A vehicle could receive a false message regarding a road closure and be forced to travel in an area that is not safe. There could also be scenarios where the vehicle needs assistance on the road (possibly if there‟s a flat tyre or hijacking) and a malicious user could prevent the message from being sent to the necessary authority. Introducing silent periods are a solution for this [**85**], as nodes are not able to access any online network during a certain period and can therefore not be attacked via software. Freudiger et al. [**87**] propose another method for counteracting malware; where a user is „warned at every access‟ to the internet. This ensures that internet access is controlled and malware cannot schedule unauthorized connections to the internet. This is however not suitable in a VANET because it becomes hazardous for drivers to read each message and consent to a connection to the internet while driving.

Chaurasia and Verma [**81**] state that in order to preserve privacy, a pseudonym system must prevent credential forgeability and disallow usage of false certified pseudonyms by a user. This implies that a vehicle must not be allowed to use a certified pseudonym that does not belong to that vehicle. Another requirement to maintain privacy is that the transaction of obtaining and the process of switching pseudonyms should not reveal the identity of the user or link pseudonyms to each other [**81**]. There are various pseudonym generation and reuse methods which are discussed in sections 2.2 and 2.3 and these incorporate mechanisms to preserve privacy while obtaining and changing pseudonyms.

According to Schaub et al. [**69**], which describes some privacy requirements for vehicular communications, identity resolution has to be supported with anonymity. This is supported by Samara et al. [**70**] and others in [**71**] [**88**], and effectively means that an authority needs to be able to link a pseudonym to a vehicle. The fuel shortage example described above is a scenario in which the vehicle can only be safely assisted if its permanent identity is known to the authorities; hence the user needs to be identified by an authority. In order to ensure that the permanent identity can be trusted, it needs to be authentic. The authors of [**77**] also employ authentication to ensure that vehicular communication is trusted and secure. Certification is the method used to ensure authentication and is discussed in section 2.1.

2.1 Certification

Certification stems from authentication, which as indicated by Diffie and Hellman [**89**] is one of the fundamentals of cryptography. According to Aziz and Akbar [**90**], a commonly stated objective of cryptography is to allow for two entities to communicate over an insecure channel (for example a telephone line or computer network) such that an opponent cannot understand what is being said. This implies that the information should be made useless to an opponent [**89**]. Swanson et al. [**91**] maintain that cryptography consists of both encryption (converting ordinary information into unintelligible information) and decryption (the reverse of encryption).

Schaub et al. [**69**] states that in order to ensure that there is accountability in a network, authentication is required. Authentication is commonly provided through certificates [**90**], and is one of the fundamental tenets of security. The following list describes authentication and the other fundamental tenets of security:

- Authentication: determining that the message is from who it claims to be from; hence assuring that the origin is correctly identified [**43**], and in turn implying integrity [**11**]. Stallings [**92**] is of the opinion that authentication is a critical component of accountability.

- Confidentiality: ensuring that information is not read by malicious users and only the authorized parties can view the information [**43**]. Kotzanikolaou and Douligeris [**93**] explain that confidentiality is where the message content is protected from all users other than the ones intended by the legal owner of the information. Confidentiality needs to be considered for two points in time: one is when data is

moving between the sender and receiver and the other is when data is received and retained by either the sender or receiver [**92**]. Confidentiality is provided by encryption in PKI systems.

- Integrity: ensuring that system assets and transmitted information is not altered by malicious users [**43**]. Integrity can be classified in terms of the following properties: no improper modification, no unauthorized authentication and no undetected change [**92**]. It therefore refers to data being conserved with regard to its meaning, completeness and consistency.

- Availability: ensuring that a system is operational and functional at a given moment [**43**]. It ensures that there is timely and uninterrupted access to the information and the system [**92**].

- Non Repudiation: ensuring that the sender of a message cannot deny sending the message [**43**].

- Privacy: ensuring that nodes have the right to control what information is given out about them, who receives the information and what purpose it is used for [**43**]. This protects the user‟s private information and identity [**92**].

- Accountability: Enables tracing to entities responsible for certain actions. Responsibility is assigned to the user for the consequences of using certain resource or information. Accountability requires the ability to uniquely determine who an entity is (identification) and the authentication of a user [**92**].

In a PKI system, users communicate securely through use of a public-private key pair. The public key is known publically and the private key is kept secret. Blumenthal [**44**] states that private keys are by definition kept secret and are used for signing messages. Public keys are used to encrypt messages so that only the user with the corresponding private key may read the message content. This works because the public and private keys are mathematically linked, and even though the public key is known, it is infeasible to calculate the private key from the corresponding public key [**44**].

A certificate is an electronic document which uses a digital signature to bind a public key to an identity [**49**], ensuring authenticity of the certificate‟s owner. The CA is the trusted

authority in the network, and is responsible for handing out the initial authoritative information: the certificate. The CA is therefore responsible for certifying a cryptographic link between the identity of a certified entity and the certified entity‟s public key [**93**]. According to Blumenthal [**44**], the CA achieves this by wrapping the certificate with its private key; thus forming the CA‟s signature on the certificate. The CA‟s signature on a certificate ensures that only the CA could have created the certificate, because only the CA holds the private key that created the certificate [**43**]. The user is considered authentic once the user‟s public key can be derived from the certificate and it can be verified that the node is who it claims to be (this is illustrated in figure 2-1).

Signing with the private key is a basic way for nodes to communicate securely as modification and forgery attacks can be defeated [**77**]. Modification and forgery attacks aim at editing/forging data but become very difficult when the data has been signed. Barker [**43**] maintains that this is because once any modification to the signed content occurs it no longer has the original signature and does not maintain integrity or authentication. After messages have been tampered with, they will not be wrapped with the same signature as that of the original message. This is because the malicious user who tampered with the original will not be in possession of the victim‟s private key.

Some of the information contained in a typical certificate, mentioned in [**49**], is listed below:

- Version number of the certificate format
- Serial Number: A unique number used to identify the certificate
- Subject: The user the certificate belongs to
- Signature Algorithm: The algorithm that was used to create the signature
- Issuer: The entity who issued the certificate; this is the TTP
- Validity Period: The time or date the certificate is first valid from and the expiration time or date
- Unique identification of certificate holder: Identification of the user, most critically, the user‟s public key.

The CA wraps a user‟s public key and other information using its private key (i.e. signed with the CA‟s private key) to produce the certificate. This ensures that by using the CA‟s public key it will unwrap the certificate and prove that it was created by the CA and can be considered trusted. The unwrapping of a certificate held by Node A is shown below:

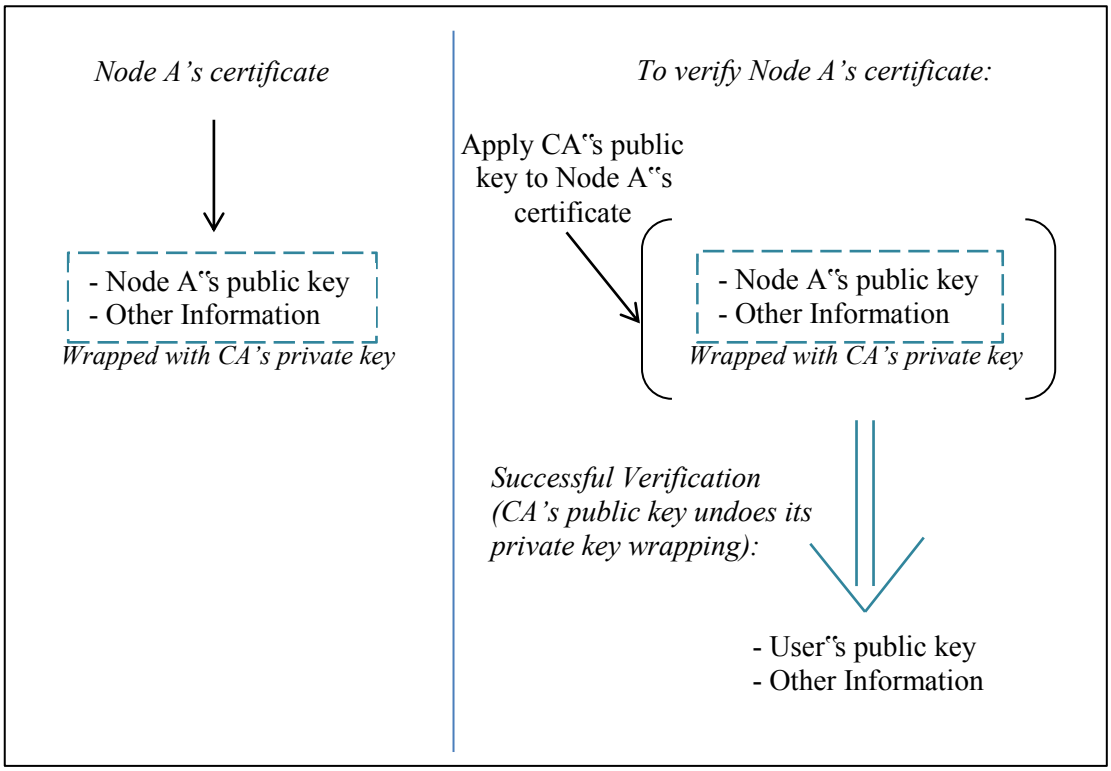

Figure 2-1 - Diagram showing how a certificate is verified

As can be seen in figure 2-1 above, the CA's public key can unwrap the signature on the certificate. Hence, Node A's certificate is considered trusted. Since only the CA is in possession of its private key, only the CA could have created the certificate. So far, only the certificate made by the CA has been opened. The certificate could be plain worthless information and would still unwrap to some value with the CA's public key. Even if the certificate after unwrapping has some content that verifies that it was a true certificate, there is no indication that it really belongs to Alice (Alice is the sender and Bob is the receiver). Further transactions are therefore required; Stallings [**92**] presents the following transactions:

Assuming Alice and Bob want to communicate and have retrieved each other's public keys from their certificates (PU_A is Alice's public key and PU_B is Bob's public key)

1. Alice uses Bob's public key to encrypt a message to Bob containing an identifier of Alice (ID_A) and a nonce (N_1), which is used to identify the transaction uniquely. The following is sent to Bob:

$$E_{PU_B}(ID_A, N_1)$$

The operation E is the encryption operation, which is performed using the operand in the subscript, on the expression within brackets.

Bob receives the message and decrypts to retrieve ID_A and N_1:

$$D_{PR_B}\big(\, E_{PU_B}(ID_A, N_1)\big) = \; ID_A, N_1$$

The operation D is the decryption operation, which is performed using the operand in the subscript, on the expression within brackets.

2. Bob replies with a message to Alice encrypted with Alice‟s public key and containing Alice‟s nonce (N_1) together with a new nonce generated by Bob (N_2). The following is transmitted to Alice:

$$E_{PU_A}(N_1, N_2)$$

Since only Bob could have decrypted Alice‟s message in (1), the presence of N_1 in message (2) assures Alice that the correspondent is Bob.

3. Alice returns N_2, encrypted using Bob‟s public key, to assure Bob that its correspondent is Alice. The transmitted content is thus:

$$E_{PU_B}\,(N_2)$$

4. Alice selects a secret session key K_S and sends the following to Bob:

$$M = E_{PU_B}\big(E_{PR_A}(\, K_s)\big)$$

PR_A is Alice‟s private key.

5. Bob calculates $D_{PR_B}\,\big(D_{PU_A}(\, M)\big)$ to recover the secret key

The result is that both Alice and Bob have verified that the public keys belong to each other and that they are communicating with the correct user. They also have exchanged a session key K_s, which can be used for the duration of the conversation. According to Zhang et al. [**94**], the objective of the session key is to allow for both users (Alice and Bob, in this case)

to possess a key that is used for encrypting and decrypting data for the duration of the conversation, and should be kept private. It is an important process in constructing a secure data communication [**94**]. These transactions above ensure both authentication and confidentiality [**92**]. Both Alice and Bob have verified that the recipient is who they claim to be, thus ensuring authentication. Confidentiality is provided by the session key as can be seen in the transmitted messages shown above, which only Alice and Bob could have read. Upon successful verification of the certificate it is considered trusted. The CA thus provides an authentic and trusted signature. In order for privacy to be implemented in a trusted network, pseudonyms need to be certified by a trusted authority. A pseudonym without certification could have been produced by any entity and could be malicious. However, using certified pseudonyms ensures that there is an authority who knows that the node is registered and can trace the node in the event of malicious behaviour [**61**]. The CA is such an authority and is commonly used to certify pseudonyms as mentioned in sections 2.2.2 and 2.2.3.

Fuentes et al. [**71**] state that certified pseudonyms are essential for providing privacy and authentication. This is also highlighted by Calandriello et al. [**61**]. Certified pseudonyms have certificates that have been produced by an identity authority (namely the CA) and that bind a pseudonym to a public key [**71**]. This ensures that the pseudonym has been certified by the CA and it is therefore considered trusted. The certified pseudonym is different from any pseudonym, as pseudonyms are merely a false name and are not authenticated in any way. The pseudonym itself can therefore not offer the security (in terms of authentication) as that offered by a certified pseudonym.

Due to the mobile nature of the VANET nodes, the CA may be unavailable at times; implementing privacy and authentication is thus prone to difficulties. The pseudonym generation methods discussed below aim at providing pseudonyms and two of these methods (sections 2.2.1 and 2.2.4) cater for when the CA is unavailable. The pseudonym reuse methods mentioned thereafter aim to allow re-use of these pseudonyms in such a manner as to not compromise the vehicle‟s privacy.

2.2 Pseudonym Generation Methods

Fonseca et al. [**64**] and Papadimitratos et al. [**88**] are of the opinion that if the real identity of a vehicle is unknown it is difficult to determine the message origin. Anonymity is essential in VANETs, as per the reasons already provided. According to Schaub et al. [**69**]

it is necessary to ensure that the pseudonym is authentic and can, if necessary, be traced back to the true owner by the CA. The methods in which pseudonyms are produced and certified are important in determining whether a pseudonym can be trusted.

Methods in which certified pseudonyms are generated and authenticated vary, depending on the function or needs of the network. There have been four main pseudonym generation approaches found in the literature:

- Pseudonyms are created by a distributed authority or the node itself and certified by the distributed authority: In this scenario the CA is available initially at setup, and is thereafter unavailable.
- Pseudonyms are self-generated and sent to the CA for certifying
- CA generates a set of pseudonyms, certifies them and hands them to the nodes
- Pseudonyms are created and certified by a node while the CA is not available. This is termed the modified pseudonymous authentication approach.

The distributed authority and modified pseudonymous authentication approaches aim to cater for situations where the CA is unavailable whereas for the remaining 2 approaches, access to the CA for pseudonym certification is necessary. These methods are discussed in greater detail below.

2.2.1 Pseudonyms Generated and/or Certified by a Distributed Authority

One scheme for providing certified pseudonyms that cater for the situation where a trusted third party is not going to always be available is that given by Weber and Stephan [**95**]. In this method, a certain group of nodes are assigned a special level of authority, making it possible for them to perform certain CA functions so that the network is able to function in the absence of the CA. Here, each network node is given a pseudorandom number generator which the CA primed with an initial seed when it was present during initialisation. Thereafter for each random number, randomization factors are used to calculate tracking pseudonyms. The randomization factors link each pseudonym and a select group of nodes are equipped with the ability to track the user‟s real identities based on the initial number fed into the random number generator by the CA. Here, the selected group of nodes form a distributed authority and are able to perform the CA‟s task of tracking the real identity of users. This scheme also allows nodes to authenticate

themselves and this further reduces the CA‟s tasks. The network is therefore designed to exist while the CA is absent where nodes take care of authentication and a distributed authority handles tracking a node‟s real identity. The distributed authority will not however provide identity authentication, making this scenario unsuited for use as a trusted network.

There is another more commonly used method for providing authentication in a distributed authority: group signatures. Group signatures, which were introduced by Chaum and van Heyst in [**96**], provide signers with anonymity. The goals for a group signature scheme, defined by Chaum and van Heyst [**96**] are as follows:

- Only members of the group can sign messages
- The receiver of the signature can verify that it is a valid signature of that group, but cannot discover which member of the group made the signature

Boneh et al. [**97**] describe the group signature scheme as that where the CA assigns nodes to groups and issues each group member with a group private key for signing messages. As with the CA‟s public key, the public keys for all groups are known by the entire network. The group private key is used by all group members to sign messages. Calandriello et al. [**98**], present a typical group signature scheme. A node produces its own pseudonyms (and corresponding public and private keys) and then uses a group signing key to produce a group signature on the self-produced public keys. The pseudonym is merely a false name which has no authentication, and by signing the public key associated with a particular pseudonym, the pseudonym is thus certified [**71**]. In this case, the node is a member of a specific group and uses its group signing key to sign the self-produced public key. This ensures that the pseudonym can be produced and signed while the CA is unavailable [**98**]. The CA ultimately decides who the group members are. When a message is transmitted, the message, message signature, certified pseudonym public key, group public key and group certificate are sent. The message signature verifies the authenticity and integrity of the message, as it is able to prove that the message came from the specified user and has not been altered during transmission. The pseudonym public key is used to verify the message signature, and is the public key associated with a particular pseudonym. The group certificate provides authentication of the group public key, which is used to verify the signature on the certified pseudonym public key. The group certificate is produced by the CA and handed to the node; it is considered trusted as the CA has signed the certificate. The CA‟s public key is known to all nodes and can be used to verify the group certificate. The issue is that group signatures have the effect of making the group more anonymous,

but the individual loses its traceability. This means that even though the group identity is not protected (as the group public key is known and all group members will carry the same public key) the personal identity is, because it is not possible to determine which node in the group the message has come from. This becomes dangerous when there is a malicious user in a group because it is not possible to determine which node compromises the group. A malicious user may give out the group signing key for personal gain. It compromises the entire group but cannot be traced to the malicious user.

In this type of pseudonym generation mechanism, the nodes form into groups that perform pseudonym generation and/or authentication tasks after initialisation has taken place with the CA present. The authentication function of the CA is thus greatly reduced catering for the common VANET scenario where the CA is unavailable at times. The distributed authority and/or group signature schemes are however not a suitable solution for the situation where a trusted network is required, because total trust cannot be present when nodes handle CA functions in the absence of the CA. This means that there are no identity authentication and hence no real trust. According to Fuentes et al. [**71**], when the CA has decided (with a sufficient amount of proof) that a node has become malicious, the pseudonym is black listed by the CA; it is added to a list containing revoked certificates. The blacklisting is based on reports of a node behaving maliciously and confirmation by the CA that the node is malicious. The revoked certificate list is trusted as it is issued by the CA. This revoked certificate list can become large due to the many pseudonyms that nodes can have, and since single nodes may be mobile and have small memory they may not have the capacity to hold large certificate revocation lists [**71**]. In order to cater for authenticity, the revoked pseudonyms must be known because even if a certificate is valid it may belong to a malicious node. Memory requirements are not a major concern in VANETs as vehicles allow for more storage capacity than typical small mobile nodes. However, the trust issues posed by distributed authorities make them an unsuitable solution. A concern for implementing this approach in VANETs is the strategy used to assign nodes to groups. Possible strategies could be groupings based on home location, driver‟s age or vehicle model. This seems to be unreasonable as VANETs are very large networks and coordinating these groups may be difficult.

2.2.2 Self-Generated Pseudonyms Certified by the CA

This scenario is where the user generates pseudonyms on its own and thereafter sends these to the CA for certification. This scenario addresses the issue of certifying pseudonyms that

have been produced by a source other than the CA; namely the nodes themselves. The following diagram illustrates the scenario; Node A sends its self-produced pseudonyms (and information identifying itself) to the CA and the CA returns the certified pseudonyms:

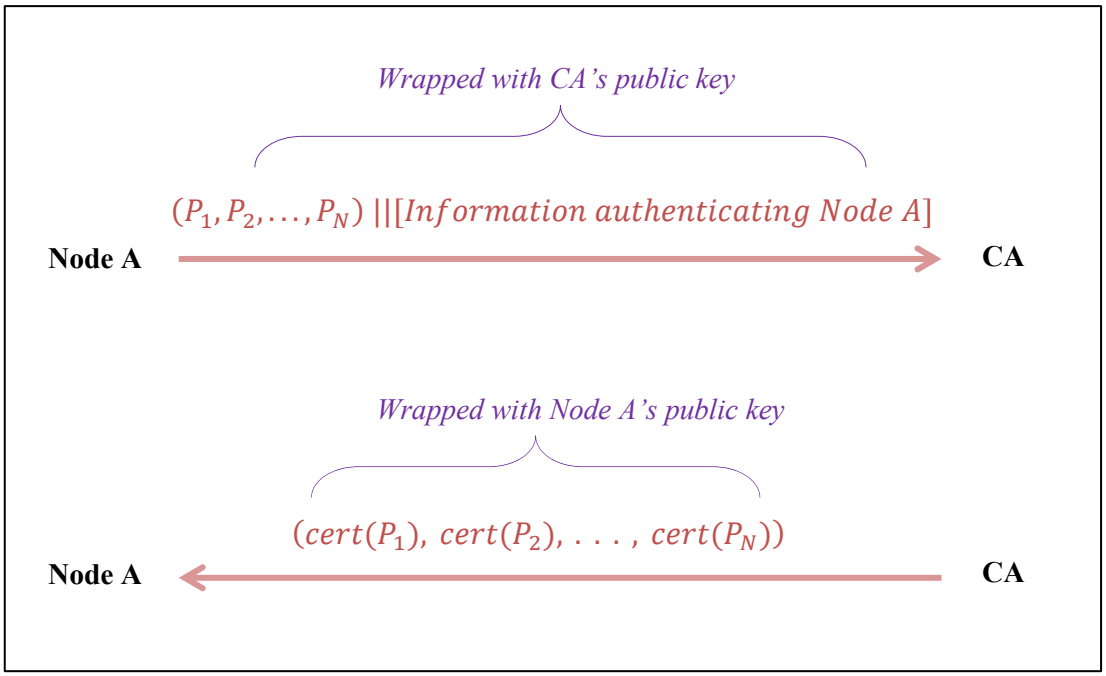

Figure 2-2 - Diagram illustrating self-generated pseudonyms sent to the CA for certification

An example of this scenario is proposed by Armknecht et al. [**99**]. The user is first responsible for authenticating itself to the CA, ensuring that the CA knows the user is who they claim to be. Thereafter the CA issues a master certificate to the user; this is to be used to authenticate the user at a later stage. The user produces its own pseudonyms, which at this point are not certified by the CA and are therefore not authentic. The pseudonyms must be sent with the master certificate to the CA for pseudonym certification. This information has to be seen by the CA only and is therefore wrapped with the CA‟s public key. This is indicated by the first transaction in figure 2-2. Upon certifying and recording necessary details, the CA sends the certified pseudonyms to the node (this refers to the second transaction in figure 2-2). These certified pseudonyms are private information because they contain false identities that the node will use to communicate. The CA therefore wraps it with Node A‟s master public key. The pseudonyms at this point carry the CA‟s signature and are authentic; these are now trusted pseudonyms. Armknecht et al. [**99**] show that it is possible for the vehicle to generate 2^{170} certified pseudonyms, which they claim to be practically infinite. From their conclusions, it can be seen that there is a high success ratio

(almost 100%) when access to the CA is available, because certificate requests are granted whenever the CA is present.

The advantage with this scenario is there is no computational burden on the CA/other trusted network entity to produce pseudonyms, as they are produced by the user [**99**]. However, online access to the CA is required for certification. This solution may be disadvantageous, depending on the pseudonym reuse strategy employed. If pseudonyms can only be used once then more need to be requested for in order to continue communicating. Thus when a node has run out of certified pseudonyms and is not in the vicinity of the CA, the node cannot communicate because there are no certified pseudonyms left. However, if pseudonyms can be used more than once, the node will be able to communicate even when there is no access to the CA.

To address the issue of requiring access to the CA for certified pseudonyms, the scheme proposed by Klaus et al. [**10**] allows a node to request for the next set of certified pseudonyms while still using a current set. This helps in the situation where the CA is not present and a node has run out of certified pseudonyms. However, this increases the amount of storage space required as the node will now store two certified pseudonym sets. This is problematic because the node is mobile and may not have a large amount of storage space. This is also a facile suggestion as it is identical to increasing the number of certified pseudonyms issued at one time. The amount of certified pseudonyms stored by the node merely increases to double the initial amount.

Hildmann and Wilke [**100**], provide a similar method, allowing for pseudonyms to be self-produced and sent to the CA for certification; they term this the pseudonymous authentication approach. It make use of the same principle as that depicted in figure 2.2. A mapping between the long term key pair and permanent identity of the vehicle is kept by the CA, which allows for tracking the vehicle. According to Dawoud et al. [**101**], this pseudonymous authentication approach is the most widely used solution to handle the trade-off between authentication and privacy in VANETs. The pseudonymous authentication approach ensures authentication, integrity, non-repudiation (where only the CA can perform the trace back to the node) and privacy.

These pseudonym generation schemes that require CA access have the flaw that online access to the CA is required when requesting for a new set of certified pseudonyms. An additional flaw with schemes in this section (and for schemes of section 2.2.3) is that the

mobile nodes will have to store the certified pseudonyms. This storage requirement places a burden on the mobile nodes. This storage capacity issue does not however affect VANET nodes.

2.2.3 Pseudonyms Generated and Distributed by the CA

Eckhoff et al. [**84**] and Fonseca et al. [**63**] maintain that a method widely used to ensure that the CA‟s signature is used to certify pseudonyms is for the CA to hand a set of pseudonyms to a node. There are variations of this, which are discussed in this section.

Examples of a variety of papers that this method has been used in are: Klaus et al. [**10**], Eckhoff et al. [**84**], Gerlach [**74**], Fonseca et al. [**63**], Freudiger et al. [**102**] and Eichler [**103**]. Gerlach [**74**] maintains that this is a common method because the certified pseudonyms have the advantage of providing both authenticity and privacy and are trusted. As pointed out by Yoon and Hyoungshick [**104**], it does not however cater for when the CA is unreachable and pseudonyms are depleted. The node is thus unable to request for and receive more certified pseudonyms. This is an issue of set replenishment; the node must have access to the CA for it to request a new set of certified pseudonyms. These schemes require the CA to keep a mapping between all the certified pseudonyms it assigned to a node and the node‟s permanent identity [**63**]. This mapping allows for the certified pseudonym to be traceable. If there are a large number of registered nodes which would probably be the case if all vehicles on the road became registered VANET users, the CA would require a large amount of storage space. Assume that each vehicle has 100 pseudonyms, where each pseudonym occupies 100 bytes and that there are 1 billion vehicles registered with the authority. The authority needs approximately 10 TB (10^9 x 10^2 x 10^2 bytes) of memory. This is not a problem as even a worldwide authority could readily have the required storage capacity for this.

A proposal by Heesook et al. [**7**] tries to fix the storage capacity issue in those instances where node storage capacity is a problem, by allowing for nodes to generate their own pseudonyms. This then becomes the same as the method discussed in section 2.2.2.

The CA is able to keep a record of the mapping of vehicle identity to the set of certified pseudonyms. An attempt to eliminate the need for mapping vehicle identity to the set of certified pseudonyms is presented by Calandriello et al. [**98**]. Here, the scenario of the CA handing a set of pseudonyms to nodes is combined with the group signature concept

(explained in section 2.2.1) to produce a hybrid scheme; nodes produce their own pseudonyms and have them signed by certain nodes which form an authoritative group. The CA assigns the authority to nodes, although they are normal mobile nodes and have the potential of turning malicious. This method is similar to the group signature scheme discussed in section 2.1.1 and is not considered secure as the trust offered by the CA is not present, and malicious nodes could be present in the group assigned to sign certificates. The community of nodes is also large and transient; for example out of a million vehicles in Johannesburg, any node will seldom have more than a hundred nodes in range, which is a very small proportion and is unlikely to contain authoritative nodes.

Soh and Sunnadkal [**105**] propose a method to reduce the computation performed by the CA when producing pseudonyms. Here, vehicles have a permanent and a temporary identity, where the permanent identity is issued by the vehicle manufacturer and the temporary identity is the generated pseudonym. This is the temporary identity the vehicle uses when communicating with other vehicles. A set of public-private key pairs are produced and sent to the CA with the vehicle‟s permanent identity; the CA verifies the key pairs, produces a pseudonym for each key pair, certifies the pseudonyms and sends them to the vehicle. This is however just a minor variant of other schemes where the node produces its own set of pseudonyms and has them certified by the CA. In this case, even though the node is producing public-private key pairs, the CA still undergoes computational burden by verifying keys, producing pseudonyms and certifying the pseudonyms. The burden placed on OBU‟s decreases. As a reminder, OBU‟s are units contained in each vehicle that are equipped with on-board sensory, processing and wireless communication modules [**57**] [**61**]. The decrease in burden on the OBU is because the processing it has to undergo is lesser than that where the pseudonyms are produced by the nodes (section 2.2.1 and 2.2.2).

In [**77**], which is a book describing VANETs and their applications, the idea of a permanent identity and short term identities is extended. Here, the CA hands out a permanent certified identity to nodes and a Pseudonym Provider (which is a TTP) hands out certified pseudonyms to nodes. The Pseudonym Provider is a trusted entity and certified pseudonyms received from it are therefore considered trusted [**77**]. The vehicle receives certified pseudonyms upon proving that it is registered with the CA; the permanent certified identity is evidence of this registration. The long term identity is not used to provide secure communication with other vehicles as it contains the real identity of the vehicle and merely serves to authenticate the vehicle [**77**]; for secure communication certified pseudonyms have to be used. This scenario is however the same as using a larger

CA, as it is essentially adding another processor to the CA. In this scheme, the CA provides authentication for users through the permanent certificate and the Pseudonym Provider issues certified pseudonyms. The CA functionality in the scenario where pseudonyms are generated and certified by the CA is thus essentially split between the CA and the Pseudonym Provider. The vehicular node functionality which can also be applied to the schemes proposed by Armknecht et al. [**99**] and Sunnadkal at al. [**105**], is shown below:

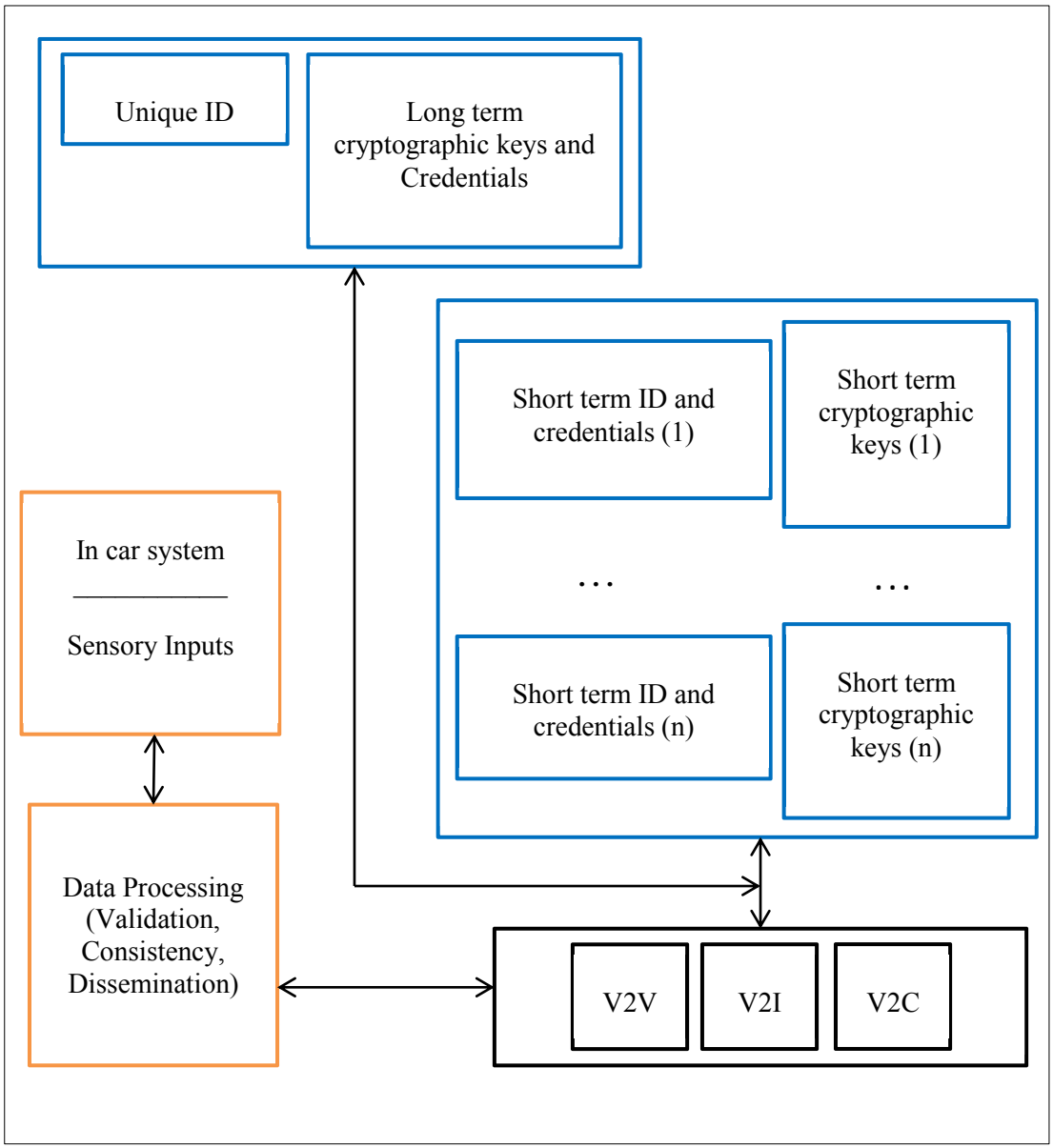

Figure 2-3 - Conceptual Secure Vehicular Communication View: Node Functionality [77]

The blue blocks in the figure above show that the vehicles have two types of identities and cryptographic key pairs; long term and short term. The types of communication in a

VANET have been defined in Chapter 1. As a recap, they are V2V (Vehicle to Vehicle), V2I (Vehicle to Infrastructure) and V2C (Vehicle to CA). The long term key pair identifies the vehicle‟s permanent identity and the short term key pairs identify the certified pseudonym. The short term identities (or certified pseudonyms) are used to provide privacy. The vehicles receive certified pseudonyms from the CA, or a TTP as in the case of [**77**]. Since these certified pseudonyms carry a trusted signature, they are authentic and meet their goal of providing privacy.

This scenario presented in figure 2-3 is a secure system in that it provides both authentication and privacy; however access to the CA/TTP is necessary to request for new certified pseudonyms. As discussed in section 1.2, in high density urban areas there is a high probability that access to the CA is always available and this scenario poses no problem, but on long distance drives and in rural areas the CA may not always be available. In the case where the CA is unavailable, which affects any pseudonym scheme requiring CA access for certified pseudonyms, upon running out of certified pseudonyms the node can only request for more once in the vicinity of the CA.

Even though access to the CA is required for requesting pseudonyms, this method is secure in that it provides both authentication and privacy. It has also been found to be the most frequently used pseudonym generation method. This is evidence that there is merit in this scheme.

2.2.4 Modified Pseudonymous Authentication Approach

The Modified Pseudonymous Authentication approach proposed by Dawoud et al. [**101**] aims at providing a method to cope with the issue of the unavailable CA. The aim is to set up a system whereby the local OBU does the generation of certified pseudonyms without the interaction of the CA.

The solution differs from the pseudonym generation methods above as it involves producing certified pseudonyms using only the OBU, as and when needed. The CA stores a certificate, which consists of two parts (the authenticator and certificate), in the OBU. The function of the authenticator is to authenticate the vehicle and the certificate (referred to as the „pseudonym certificate‟ from hereon) authenticates the authenticator. The authenticator is embedded within the pseudonym certificate, shown graphically below:

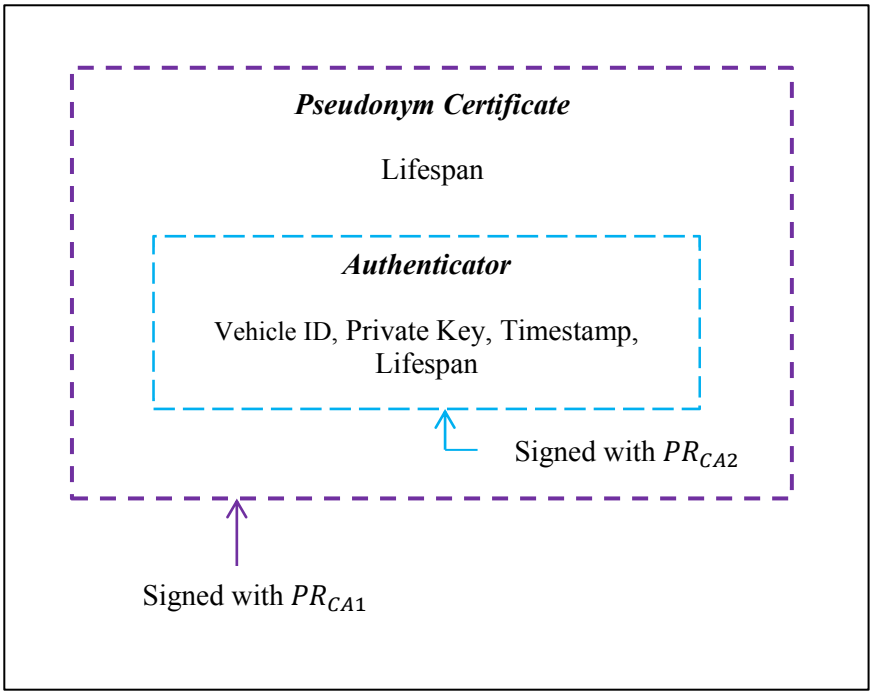

Figure 2- 4 - Certificates used in the Modified Pseudonymous Authentication Approach

The important attributes contained in the pseudonym certificate are the lifespan of the certificate and the authenticator (shown in figure 2- 4 above). The lifespan is necessary to determine if the pseudonym certificate is valid. Validity information is critical as an invalid certificate cannot be trusted. The scheme allows for the CA to have two public-private key pairs, referred to as the CA"s first public-private key pair and the CA"s second public-private key pair. The pseudonym certificate makes use of the CA"s first public-private key pair (PU_{CA1}, PR_{CA1}). PR_{CA1} is used by the CA to sign the pseudonym certificate. The authenticator is part of the vehicle"s pseudonym certificate. Each time a pseudonym is used, the pseudonym certificate changes but the same authenticator is embedded in it.

With reference to the figure above, the important attributes in the authenticator are the vehicle permanent identity, user"s private key for pseudonym calculations, timestamp and lifespan. This information forms a „permanent certificate" for the vehicle, as the vehicle"s permanent identity and secret key is authenticated though the authenticator. The timestamp and lifespan provide validity information and are used to determine if the vehicle"s permanent identity is valid. The authenticator makes use of the CA"s second public-private key pair (PU_{CA2}, PR_{CA2}). This differs from the conventional PKI scenario (defined in section 2.1) because here both PU_{CA2} and PR_{CA2} are kept private. The CA signs the

authenticator with PR_{CA2}, and since PU_{CA2} is not known to other entities, only the CA can verify the signature created by it on the authenticator. PU_{CA2} is used in instances where the CA has to link the permanent identity to the user [**101**].

The scheme allows for each pseudonym to be calculated by the node using a procedure that is based on the user‟s private key and a sequence number [**101**]. The sequence number keeps track numerically of which pseudonym the current one is. The scheme allows for the pseudonym‟s public key and sequence number to be attached to the pseudonym certificate, and sent to other nodes. The pseudonym certificate contains information to prove that the user is registered with the network. The authenticator, which is within the pseudonym certificate, carries the vehicle‟s permanent identity. This is seen by other nodes as unintelligible information, ensuring that the authenticator can always be traced to the vehicle by the CA and not by other nodes. The CA is able to track the pseudonyms because the algorithm used to generate key pairs relied on the approach (El Gamal), a key and the sequence number. This way, using the vehicle‟s long term key pair and the sequence number, the CA can verify the vehicle identity and the pseudonym.

This method functions well to save storage space at the OBU, as pseudonyms are created as and when needed and the CA need not be available for certification. The vehicle is therefore able to communicate in areas where there is no CA. The method has been analyzed by the authors in terms of storage area needed, communications with the CA and Non-repudiation; these are presented below:

- Storage area needed: There is no need to store any certified pseudonyms in the OBU or at the CA, as the message keys are calculated on demand [**101**]
- Communications with the CA: There is no communication between the vehicle and CA during normal operation [**101**]. The keys used for communication are self-generated and there is no need to send them to the CA for certification. The CA is however contacted when the need to verify a pseudonym certificate or to trace a node arises.
- Non-repudiation: The presence of the authenticator guarantees that the sender can be traced [**101**].

This scheme however allows for the private key and vehicle identity contained in the authenticator to be monitored. This is because the confidential information contained within the authenticator does not change with each pseudonym and as a result the same

information will always be carried with the pseudonym certificate. Even though no other entity can view the contents (because the CA‟s second public key is needed to unwrap the authenticator and it is kept private) this authenticator information always remains constant, allowing for the vehicle to be traced. Pseudonyms will be changing but the same authenticator will be sent and the vehicle can thus be traced. This method attempts to provide privacy and authentication but is not successful. Other means of ensuring that the confidential information contained within the authenticator does not allow for tracing the vehicle must therefore be introduced.

2.3 Pseudonym Reuse Methods

The pseudonym reuse methods are critical for the privacy of the system [**88**]. These are methods in determining when the pseudonyms are changed and whether or how often they may be re-used. Chaurasia et al. [**72**] are of the opinion that regular pseudonym change is necessary because the same false identity cannot be retained for too long. Pseudonym change has also been identified as a requirement by Eichler [**103**]. This is because continually changing pseudonyms conceal the real identity of a vehicle by de-linking the source of messages to its original identity [**72**]. Weerasinghe et al. [**19**] and Kargl et al. [**75**] identify the risk that certified pseudonymous samples can be collected and combined to form pseudonymous location profiles. A malicious node that develops these location profiles could easily relate them to specific vehicles. Off-line information could be obtained via cameras and profiles could be correlated to specific areas; for example profiles starting/ending on weekday mornings at the same location would likely reveal home and work addresses that could then be connected to individuals [**75**]. Kargl et al. [**75**] therefore conclude that the use of a single pseudonym is not enough to protect privacy. Gerlac and Guttler [**79**] propose that each vehicle needs to thus use multiple pseudonyms, changing between them regularly using some time schedule or other scheme.

Pseudonym change mechanisms are needed in each of the pseudonym generation methods above. The following pseudonym change mechanisms are discussed in this section:

- Changing Pseudonyms Randomly
- Geographic Change in Pseudonyms
- Changing pseudonyms after a Specified Time Interval

Pseudonyms can follow either a single use or a multi-use strategy. The single-use pseudonym strategy is the ideal where the pseudonym is used only once and as a result the vehicle cannot be tracked at all. This does not compromise the vehicle"s privacy although the problem that may result is the cost to produce pseudonyms. The question then becomes, is the pseudonym used for one message only or one conversation. Evidently, in those situations where there is a conversation or bidirectional communication between two nodes, the pseudonym must remain constant for the entire conversation. Hence, using pseudonyms multiple times (the multi-use pseudonym change strategy) is therefore better suited for VANETs, but results in privacy issues. Here, the same pseudonym is used more than once, allowing for a conversation to be easily held between two vehicles. This is advantageous because if the CA is not reachable or the vehicle was not used for a longer time period the vehicle will not run out of certified pseudonyms because it is able to reuse the previous pseudonyms [**84**]. It however hinders privacy as it is known both instances of use of the pseudonym were from the same vehicle. The vehicle can therefore be tracked. The fact that VANETs have a highly dynamic environment makes this tracking difficult, because the next time the same pseudonym is used might be when the vehicle is in an entirely different environment. There is also a high likelihood that malicious nodes will not know in which vicinity a vehicle will use its pseudonym again.

There are however individuals who have daily patterns, especially in high density urban areas. There is a good chance that these vehicles will be in the vicinity of the same vehicles every day, as daily patterns of other individuals coincide. In this case, the environment does not change dynamically and it may be problematic if the same pseudonyms are used at around the same time every day. In this scenario, changing pseudonyms in a random manner has merit. Schemes in section 2.3.1 employ this method.

All the schemes in sections 2.3.1- 2.3.3 employ a multi-use pseudonym strategy. Section 2.3.2 proposes a method for lowering the possibility that pseudonyms can be linked to vehicles after being visually observed. Section 2.3.3 aims to decrease possibilities of linking a current pseudonym to previous ones. The following subsections address these methods in which pseudonym change may occur when pseudonyms are re-used multiple times, and can be used with each of the pseudonym generation methods above.

2.3.1 Changing Pseudonyms Randomly

In this scenario, nodes change pseudonyms in a random manner with the aim of increasing anonymity in instances where patterns in pseudonym usage can be developed. A pseudonym is reused a random number of times and then changed. As per the nature of random selections, these pseudonym changes do not follow any particular order and therefore future use of the pseudonyms cannot be easily predicted by other nodes [**63**]. Areas that are being monitored for patterns in pseudonym usage will now have an element of confusion for malicious users performing the monitoring.

Implementations of this scenario are presented by Fonseca et al. [**63**] and Armknecht at al. [**106**]. This pseudonym usage method also prevents linking current pseudonyms to previous ones, and using the information to predict the use of future pseudonyms. Linking pseudonyms occurs when the attributes of a pseudonym are linked to the attributes of another pseudonym used by the same vehicle. This may be done using the vehicle‟s speed attribute, and is explained in section 2.3.2 below.

A slight variation to this scenario is the collision free pseudonym scheme proposed by Kim and Hyoungshick [**104**]; nodes use elements from a permutation matrix held by the CA to determine the next pseudonym. The elements from the permutation matrix can be re used and are chosen randomly. The scenario is thus also expected to be highly suited for scenarios where the same vehicles may be in the same vicinity and communicate with reused pseudonyms on a daily basis. This is because the random use of pseudonyms creates confusion and tracking is thus harder.

It is advantageous to change randomly between pseudonyms for the reason of creating difficulty for malicious nodes to analyse network traffic. Patterns cannot be easily generated and this creates confusion, which aids with ensuring that the user‟s privacy is maintained. Further, the random selection of pseudonyms can easily be implemented by the node itself with a pseudo random number generator.

2.3.2 Geographic Change in Pseudonyms

Another approach for pseudonym change is that proposed by Lu et al. [**83**]; change pseudonyms in a *mix zone*. Liao and Li [**107**] explain that this is where the vehicle enters the *mix zone* with one pseudonym and changes to a different pseudonym before leaving the *mix zone*. These *mix zones* are generally high density areas where there are many common

attributes between vehicles as well as many other vehicles going through pseudonym changes [**107**]. Since many vehicles are involved in changing pseudonyms in these *mix zones* there is an increase in difficulty of linking pseudonyms. The papers discussed in this section propose changing pseudonyms in *mix zones* as it has the effect of making it very difficult to link the pseudonym a vehicle had used before entering the *mix zone* to that used before leaving it. Pseudonyms are reused, although the pseudonym a vehicle uses at the start and end of the same *mix zone* cannot be the same, as this defeats the purpose of the *mix zone*.

Mix zones for pseudonym change are also proposed by Matthias [**74**]. The *mix zone* is presented as an area in which vehicles have common context information (information used to characterize an entity‟s situation). This context information could refer to the vehicle‟s location, and possibly velocity. There are certain areas on the road where a vehicle‟s context information will be the same as that of other vehicles (for example traffic light intersections and parking lots). According to Zhendong et al. [**108**], due to the common context information, these areas form a *mix zone* and Gerlach [**74**], Lu et al. [**83**], and Freudiger et al. [**109**] consider it safe to change pseudonyms in these areas. The reasoning used is that distinguishing between vehicles context attributes is made difficult in these *mix zones* (due to common context information) and if pseudonym changes are made in the *mix zone* the vehicle has less likelihood of being tracked. It might be possible to perform a visual check and determine which vehicle a message was sent from, for example if one vehicle is stationary at an intersection and a message was sent together with context information indicating that the vehicle is travelling at 0km/hr. and the stationary vehicle is the only stationary vehicle in the vicinity then it can be assumed with a high possibility that the same vehicle sent the message. If a parking lot is however declared as a *mix zone* there is a high possibility that there will be many vehicles with a velocity of 0km/hr. (common context information) and if a message is sent it is more difficult to link the pseudonym to the vehicle.

Lu et al. [**83**], describe the *mix zone* as a „social spot“; these are areas where many vehicles temporarily gather, for example intersections. Pseudonyms are changed at these „social spots“ in order to hide the pseudonym change process. This is done so the new and old pseudonyms cannot be linked. At these *mix zones*, the vehicles have common attributes for velocity and location (the social spot). If a pseudonym change is made when these attributes are common for many vehicles and there are many vehicles present in the *mix zone* then the scheme claims that pseudonym changes cannot be linked to a single vehicle.

In VANETs it is highly likely that malicious nodes may monitor traffic on a road to spy on vulnerable vehicles; *mix zones* function mainly to lessen the possibilities of linking pseudonyms to vehicles [**109**], making the malicious monitoring difficult.

2.3.3 Pseudonym Change after Specified Time Interval

The last category for changing pseudonyms is where all vehicles change pseudonyms after a specified time interval; this helps in ensuring that an individual vehicle"s change in pseudonyms cannot be traced. This is because all nodes change pseudonyms from the present pseudonym to a different one at the same time [**84**], making it very difficult to link a specific vehicle to its previous or current pseudonym.

In a scheme proposed by Calandriello et al. [**98**], the pseudonyms are changed after a defined period, τ; ensuring that the pseudonym change cannot be traced as all nodes change pseudonyms during this time. Similarly Eckhoff et al. [**84**] allow for vehicles to switch pseudonyms after a certain time; the node"s clocks are synchronized with GPS and one pseudonym per time interval is changed. However in both cases, if two messages are sent before the specified time (τ time units in the case of [**98**]) have elapsed, it is possible to link these messages to the vehicle. This means that the vehicle can then be tracked. Further, in the case of VANETs it is not likely that a vehicle will come into contact with the same vehicles twice in one day; hence there is no need for the pseudonym to change many times a day.

An advantage of the time-slotted approach is its property to ensure that a vehicle always has a certified pseudonym to participate in the communication as long as it has received its certified pseudonyms in the setup phase [**84**].

2.4 Conclusion

Chapter 2 initially introduced privacy and described the need for privacy in VANETs. Pseudonyms are a commonly used method for implementing privacy [**18**]. In order for pseudonyms to be authentic, they have to be signed by a TTP [**75**]. A section on certification describes what a certificate is, the need for certificates and their operation. Once a pseudonym has been signed by a TTP, it becomes a certified pseudonym.

Thereafter, four main pseudonym generation methods were discussed. Distributed authorities make use of groups for signing pseudonyms and ultimately cater for when the CA is not available to certify or authenticate pseudonyms. The CA handing out a pool of certified pseudonyms to nodes is the most widely used pseudonym generation method and offers a secure method for catering for both authentication and privacy [**74**]. It however has the shortcomings that large amounts of space are required at the node for certified pseudonym storage and access to the CA is necessary when requesting for certified pseudonyms. The method whereby pseudonyms are self-produced and then sent to the CA for certification has variations which aim at decreasing the storage capacity burden on mobile nodes. The only difference here is that pseudonyms are produced by the node; they still require certification by the CA and hence online access to the CA. The modified pseudonymous authentication approach aims to rectify both the storage capacity burden on nodes and the unavailability of the CA at certain times by allowing vehicles to produce pseudonyms as and when needed. The CA does not need to be available for communication to take place. However, the privacy of the vehicle is hindered as there is constant information that the vehicle has to send with its messages, even though pseudonyms continue to change. The vehicle is therefore vulnerable to being traced. This is further elaborated on in Chapter 3, where the proposed solution which solves this issue is developed.

Pseudonym reuse strategies aim at solving the issue of linking pseudonyms to a vehicle or to previous pseudonyms [**75**]. In a VANET it is possible to use information about the vehicle to determine which vehicle sent a message; this hinders privacy. All three surveyed reuse strategies employ multi-use pseudonyms, allowing for pseudonyms to be used more than once. Due to the fact that patterns in pseudonym usage can be formed, multi-use pseudonyms make a vehicle prone to being tracked. Changing pseudonyms randomly, geographically and after a specified time are methods that attempt to decrease the possibility of determining any link between the vehicle and pseudonym. Random change of pseudonyms help to reduce the possibility of tracking a vehicle through its pseudonyms based on patterns that may be formed through daily routines. *Mix zones* aim to prevent the link between pseudonyms and vehicles, which could be formed via visually analysing vehicles in a certain area [**107**]. Changing pseudonyms after a specified time is a method that aims at decreasing the possibility of linking a pseudonym to the previous pseudonym. It may be possible to predict the future use of pseudonyms if there are patterns observed in pseudonym usage, and this could have consequences on the privacy of the network.

3. Proposed Solution

From the preceding literature review on privacy in VANETs, we can see that the desire for privacy is directly in conflict with the need for authentication and certification that can only come about through the registration with a trusted third party or Certificate Authority. Without this registration, no node would be likely to trust the communications from any other node as there would be no way of tracing a node that gave out false information. Hence in a situation where Alice is sending some message to Bob, Bob needs to receive a certificate with Alice‟s message that would guarantee that Alice is a registered, authenticated vehicle and can be traced by the CA if the need arises. This certificate must have been signed with the CA‟s private key so that on receipt, Bob can use the CA‟s public key to check the certificate. If the certificate can be validated with the CA‟s public key then it can only have been produced by the CA and then the content of the certificate could be used to verify the registration status of Alice. However, to provide Alice‟s (and Bob‟s) privacy, each message sent by Alice should appear as if it comes from a different vehicle; Alice needs pseudonyms. For the remainder of this chapter, Alice is considered the sender and Bob is the receiver. Pseudonyms used for Alice are Carol, Denise and Emily. Bob‟s pseudonym is Dale.

From the current literature, the dominant approach, as detailed in section 2.2.3, is for the CA to generate a set of certified pseudonyms for each vehicle; the vehicle will then cycle through these certified pseudonyms according to some scheme and then, once the set is exhausted, apply to the CA for a new set. The major difficulty with these approaches (discovered in section 2.2.3) is that the pseudonym set can run out when a vehicle has no access to a CA and this may compromise privacy or even require the vehicle to stop communications, depending on the reuse strategy. It would therefore be beneficial to allow a node to generate its own authentic pseudonyms as and when needed, in the absence of the CA, while still ensuring that only the CA can trace the source.

The requirements of the system and the mechanisms employed to meet the requirements are discussed initially. Section 3.1 then develops a certificate to cater for privacy, authentication and traceability. This is followed by message transactions in section 3.2, which illustrate how the solution functions. In section 3.3, the solution is analyzed and ways in which the solution copes during certain attacks are detailed.

In order to implement both authentication and privacy, the system requires that a node is able to generate an authentic pseudonymous identity while still being traceable by the CA. Privacy is essential, as discussed in the previous chapters, and is provided by means of a pseudonym. In order to provide both authentication and privacy, it is necessary to provide nodes with a pseudonym that is authentic [**71**], hence an authentic pseudonymous identity. This means that even though the identity displayed to other users is not the user‟s real identity and has been self-produced, it should be possible to prove that the node is registered with the network, can be traced by the CA and messages sent from the node are authentic. It is possible to confirm a vehicle is registered with the network upon verifying the authenticity of its pseudonym. Identifying a link between two authentic pseudonymous identities belonging to the same node should be possible for the CA only and not for other nodes. If Alice were to send messages to Bob under the pseudonymous identities of Carol and Denise, it should be impossible for Bob to know that both Carol‟s and Denise‟s messages are from the same person, while both pseudonyms can be traced back to Alice by the CA if necessary. In order for the CA to determine that both pseudonyms belong to Alice, Alice‟s permanent identity must somehow be carried with each pseudonym, so that it can be traced by the CA. The pseudonyms are independent of the vehicle‟s real identity, and there is therefore no way of determining that Carol and Denise are both Alice unless Alice‟s identity is carried with the false identities of Carol and Denise. This however means that there will be a common part in both Carol‟s and Denise‟s certificates, which ties their identities back to Alice. The scheme developed by Dawoud et al. [**101**] is one such example where this problem exists; there is common permanent information carried with the pseudonyms, making it possible to trace the source. This compromises privacy and does not meet the privacy and authentication requirements.

In order to meet privacy requirements, a certificate containing the vehicle‟s permanent identity and pseudonym needs to be created such that only the CA can see the permanent identity and there is no link between the current pseudonym and previous pseudonyms. The CA has to thus hide the permanent identity within a certificate while also ensuring that the pseudonym currently used is certified and does not give out the permanent identity in any way. Assuming Alice wanted to communicate as Carol, the following diagram illustrates what sort of certificate is necessary:

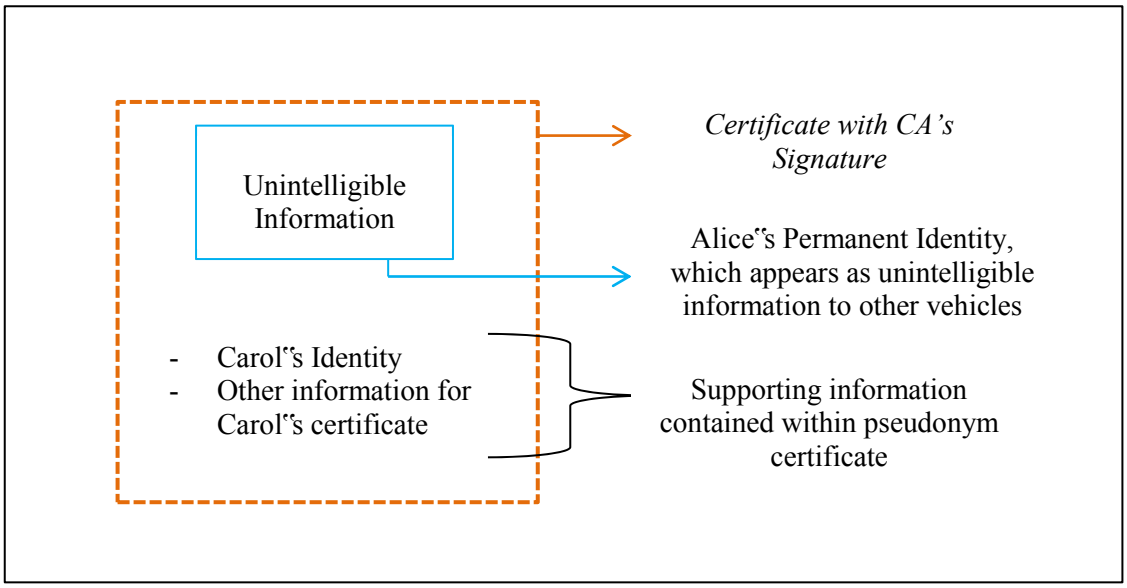

Figure 3-1 - Figure illustrating certificate requirements for privacy and authentication

The figure above shows that Alice‟s permanent identity is not readable by other vehicles; it should appear as unintelligible information. Further, the certificate needs to be signed by the CA, ensuring it has a trusted signature. This caters for both authentication and privacy, but there is still an issue. This becomes very difficult to implement in a VANET because the CA may be unavailable at times. Pseudonyms will thus need to be produced and certified while the node is offline.

In order to cater for the CA being often unavailable an option is to implement RSU‟s as proxies to the CA. The function of the proxy to the CA, according to Yap et al. [**110**], is to sign a message or certificate on behalf of the CA. This approach is presented in several papers as mentioned in section 2.2.2. A little reflection however indicates two flaws which essentially render this approach unsuitable. The first issue is that it is expected that the RSUs are always going to constitute the CA itself just as current vehicle registration offices all represent the vehicle license authority. Hence to think of them as proxies is not very sensible. The second difficulty is that it is the RSUs that may be unavailable depending on the location of the vehicle as no matter how well provisioned the environment is with RSUs, it would be impractical and maybe even impossible to ensure 100% coverage in all locations. RSU‟s are also costly to construct and can therefore not be close together. This is also why access to the RSU may not always be available.

The obvious approach is to have the CA always available to generate a pseudonym whenever required but since this is not practical, it was investigated if it is possible to have

some proxy for the CA always available at the node. For this to work, the proxy would have to be a part of the node yet must be implemented in such a manner that it would be impossible for the node to interfere with its operation or to even examine its operation. The proxy should therefore be tamper-proof. It is necessary because the proxy would be in possession of confidential information and allowing for the node or any other node to easily access the proxy will compromise the system‟s security. The proxy would have to be secure in terms of keeping private information confidential and not being easily attacked. The proxy would in essence be required to produce the certified pseudonyms and therefore need to have the ability to perform cryptographic computations. Proxies need to receive updates, etc. from the CA and therefore need online access to the CA.

A convenient method to ensure that each OBU is equipped with a proxy for the CA is to make use of smart cards. Petri [**111**] describes smart cards as small plastic devices that contain non-volatile memory and microprocessor components, capable of performing very large cryptographic computations. Smart cards are presented in greater detail in the appendix. The specific type of smart card focused on here is contact smart cards. This is the type that is used in bank cards, credit cards and SIM cards for mobile telephones [**112**]. These smart cards are rendered useless upon being tampered with and this protects confidential information that the proxy stores [**113**]. When tampered with physically, the data on the smart card is destroyed, thereby protecting the stored information. The confidential information on the card can also be protected and processed by cryptographic algorithms. This ensures that the confidential data cannot be read by malicious users and analysing the algorithm operation is difficult.

According to a study conducted by Paradina et al. [**114**], on implementing Java Card Technology on smart cards, there are more than 1 billion smart cards manufactured each year. This is due to their convenience and ability to be used on a large range of complex applications. Smart cards are described as „small computers“ by Paradina et al. [**114**], because they have 8, 16 or 32 bit CPUs, clock speeds between 5-40 MHz and ROMs of between 32 and 64 KB. To show the capability of this „small computer“, Itoi et al. [**115**] use the smart card to successfully implement a UDP/IP stack, Simple Password Exponential Key Exchange protocol, Kerberos (an authentication protocol) and SSH clients which have been modified for smart cards. SIM cards have been proposed to implement PKI functionalities by both ChunXiao et al. [**116**] and Li et al. [**117**]. In ChunXiao et al. [**116**], a SIM card generates dynamic passwords for authentication using a security algorithm that has been embedded in the SIM card. This is convenient as a user does not

need to carry separate authentication devices. Further catering for authenticating users, the scheme proposed by Li et al. [**117**] uses SIM cards to produce digital signatures; this is achieved by combining hash functions and an asymmetric encryption algorithm. These schemes are evidence that SIM cards can perform complex cryptographic algorithms and are reliable. SIM cards are a type of smart card which are widely used in cellular phones and, according to Czerniewicz [**118**], have been escalating in production in recent years. Smart cards used for internet usage are for example those used in mobile telephones that have GSM/3G capability. This allows for the smart card to receive secure information. Satisfying the requirements of a tamper proof proxy, capable of complex cryptographic computations and able to keep information secure, smart cards are thus highly suited for the task of proxy to the CA.

Since physically damaging the proxy will render it useless, tampering with another vehicle‟s proxy is not a viable option. Vehicles may however be prone to being hijacked or broken into and OBU‟s may be stolen. This is possible and therefore needs to be catered for. As soon as an OBU is stolen the CA needs to be made aware so that the unit can be blacklisted and relevant records may be updated. The CA performs the blacklisting upon verification that the victim is a registered user. Once the OBU has been blacklisted the thief will no longer be able to use the unit and send out messages with the victim‟s pseudonyms. The OBU can then be considered useless and the proxy is disabled and cannot be used. This is similar to the common blacklisting protocol followed when a mobile telephone is stolen. Some security should be implemented in order to make it difficult for OBUs to be stolen. A method could be to implement a PIN authentication system. A PIN should be entered to authenticate the user; when a user starts a vehicle they should be requested to enter a pin known only to them so they can be authenticated and activate the OBU. It makes sense to use the PIN like a car radio; it only needs to be entered on power up after which it is stored in volatile memory. This means that if the vehicle battery is disconnected or the OBU is disconnected, the code has to be re-entered on the next power up. If a thief gets hold of the OBU it is essentially useless without the PIN and pointless to steal. This is similar to the authentication used in a mobile telephone. As a mobile telephone starts up, the user is prompted to enter a PIN and the network may only be accessed once the correct code is entered. Calls, texts and internet connections can only be made if the correct PIN is entered. With the OBU, if the PIN is wrong then the OBU should not activate because it is assumed that the authorized user did not attempt to activate the OBU. In this scenario, a thief may hijack a vehicle and ask the user to enter the pin code. This is an attempt to gain

access to the OBU via the authorized user. In this case a duress code should exist to aid victims. If a certain code (the duress code) is entered as the PIN then the OBU activates and immediately sends a distress signal to the CA. The CA may then send necessary alerts to security personnel. The proxy activates, produces pseudonyms and sends messages, in order to make the thief believe that the right code was entered. The proxy should then shut down after a few pseudonyms have been used and the CA thereafter blacklists the OBU.

The CA will also blacklist the OBU if a node has become malicious. There may be many other nodes reporting that certain pseudonyms have behaved maliciously. The CA will then trace the vehicle‟s permanent identity using the pseudonyms and if it is found that in most instances it is traced to the same vehicle there is a high likelihood that the vehicle is behaving maliciously. The CA may then monitor the potentially malicious vehicle‟s proxy and read the messages sent from it to confirm the malicious behaviour. The CA could also identify a malicious node by observing irregularities in network traffic. Analysing the network traffic may be done by an external trusted source since the function of the CA is only to handle network registrations. The frequency of warning messages may be observed to have unusual spikes at quiet areas where there are no accidents on the road and no real need for warning messages. This is such an irregularity that will be brought to the CA‟s attention. The CA may then be able to identify the potentially malicious vehicle using location information provided by the trusted source. The CA could then communicate with the vehicle‟s proxy and determine if the node is indeed malicious. Once the CA has identified a node as being malicious it needs to be blacklisted. This means that the proxy must no longer function to produce certified pseudonyms and should not be able to communicate with other vehicles. The OBU is disabled so that it cannot be used. This is recorded by the CA and is done to stop further malicious behaviour. The malicious node is thereafter added to a revoked list maintained by the CA which contains the vehicle‟s and owner‟s details. The proxies cannot view the real identity of a vehicle and therefore do not need access to this list; hence this is kept only at the CA for record purposes. When a vehicle attempts to register at the CA, it is checked against the revoked list. If the vehicle‟s OBU has previously been blacklisted some sort of test to determine if there is a high possibility that the user will behave maliciously again should be done. The vehicle could be put on a trial for a few months. During this trial period, the vehicle should be made to inform the CA of new towns or cities entered so the CA may track the vehicle and determine if any malicious behaviour has taken place in these areas that could possibly be linked to the vehicle. If after the trial period the previously malicious vehicle has not

performed any harm then the vehicle may continue as normal and be left unmonitored by the CA. The proxy therefore has the ability to cope in the event of malicious use.

Utilizing these smart cards as proxies allows for the user to always have verifiable certificates for the pseudonyms produced irrespective of the vehicle‟s proximity to the CA. This is because the CA‟s proxy is always „on-board‟ the vehicle. The CA‟s proxy, which has the same level of authority as the CA, is able to issue certificates to users. The proxy would also be able to produce certified pseudonyms when required, avoiding the need to wait until the vehicle is in the vicinity of the CA, or for the CA to use large amounts of memory to store a list of pseudonyms for each vehicle.

There could be a single public-private key pair for both the main CA and proxies or separate keys for the main CA and proxy. Should there be a single public-private key pair used by both the main CA and proxies, it would not be possible to distinguish between what has been signed by the main CA and what has been signed by its proxies. The proxies would essentially have the same identity as the main CA and would therefore be able to perform tasks as the main CA. The proxies function mainly to produce certified pseudonyms and offer convenience as pseudonyms can be produced when the CA is unavailable, but are not required to perform other CA tasks. Registering users, having access to the vehicle‟s permanent identity, creating certificate revocation lists for example should all be the main CA‟s responsibility. The main CA is the main authority and performs greater functions than that of the proxy and therefore requires its own identity. The main CA thus requires a public-private key pair separate from the proxies.

Now that the proxy needs a key pair separate from the CA, the issue is whether each proxy is given its own public-private key pair or not. It is essential that a user is not able to determine which proxy produced a particular proxy signature. Identifying the proxy is the same as identifying the vehicle because each vehicle has a proxy. Allowing for this link between proxy and vehicle to be known is therefore not acceptable. By embedding the same public-private key pair in every proxy, all proxies will produce a signature using the same private key. It will therefore not be possible to determine which proxy created the signature, aiding with privacy. An advantage of using the same public-private key pair for every proxy is that computation time for the event where the main CA needs to verify proxy signatures is reduced (as there is only one public-private key pair for all OBU‟s) and the main CA does not need to use memory to store separate public-private keys for each OBU. Implementing different public-private key pairs for each proxy cannot be considered

because each proxy‟s public key will be distinct, even when pseudonyms change and this will compromise privacy as the vehicle can be traced through the proxy‟s public key. It will also be difficult to implement because every vehicle would have to store public keys for every existing proxy which could amount to hundreds of millions. There is also the issue of verifying other proxy‟s signatures. Each proxy would have to verify the public key of another proxy; this will require access to the main CA. Therefore it is far better to ensure all proxies have the same public-private key pair.

Since the CA requires a public-private key pair separate from its proxies and all proxies have the same public-private key pair, there needs to be two public-private key pairs that belong to the CA. The main CA holds both key pairs and all proxies holds one key pair. The main CA is identified by the CA‟s primary public-private key pair (PU_{CA1} ,PR_{CA1}), and the proxy is identified by the CA‟s secondary public-private key pair (PU_{CA2}, PR_{CA2}). The pseudonym produced by the proxy is therefore signed with PR_{CA2}. Since the CA‟s proxy is trusted, it is guaranteed that a signature of the CA‟s proxy is as authentic as the main CA‟s signature; hence, it can be fully trusted. The pseudonym signed with PR_{CA2} therefore provides certainty that the pseudonym belongs to a registered vehicle.

The CA‟s main public key, PU_{CA1} is part of the information that would be given to a user upon registering with the network; it is therefore known by all registered nodes. Keeping the CA‟s secondary public key, PU_{CA2} , secret will emulate the wire-line PKI model while making PU_{CA2} public will stray away from the convention. According to the PKI model, when Node A has Node B‟s certificate and would like to retrieve Node B‟s public key from the certificate, the convention is shown below:

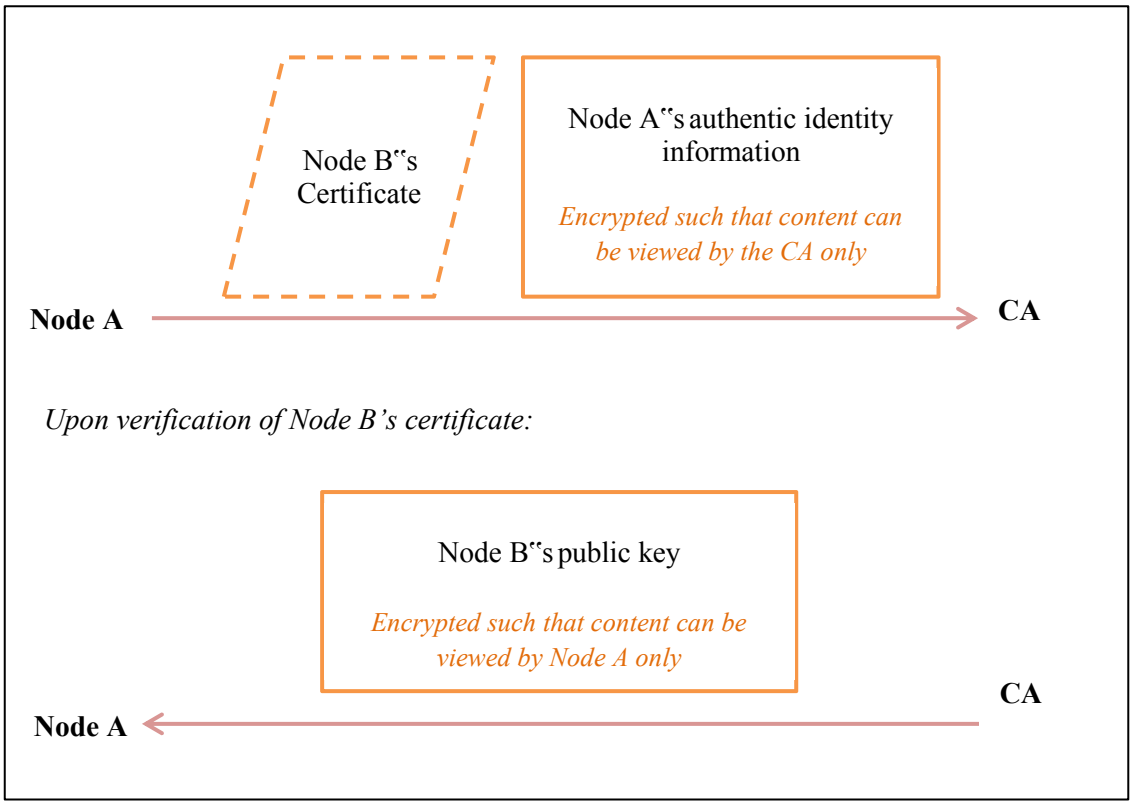

Figure 3-2 - Diagram indicating conventional PKI public key retrieval from a certificate

As can be seen in the above figure, Node A sends Node B‟s certificate to the CA (together with information authenticating Node A) and the CA verifies Node B‟s certificate. Stallings [**92**] states that if the certificate is valid the CA returns Node B‟s public key to Node A. This is illustrated by the second transaction in figure 3-2. In the same way, suppose PU_{CA2} is known only to the CA, then each time a certificate has to be verified and a vehicle‟s public key extracted from a certificate the user must send the certificate to the proxy; thereby emulating the model shown in figure 3-2. However, consideration for the OBU‟s computing power and energy consumption must be taken in account. The smart card has a small processor and cannot handle too many processes [**115**]; it should therefore not be subjected to excess strain. It is more viable for the user to verify a received certificate and extract a vehicle‟s public key from the certificate than to require the proxy to perform these computations. Furthermore, allowing the user to have access to PU_{CA2} is safe because with this knowledge only certificate verifications can be done. The user will not have access to PR_{CA2} (as this is known only to the CA and the proxies) and can therefore not produce any proxy certificates or sign a message as the proxy; hence no malicious use can come of it.

As a summary thus far, the solution therefore proposes to implement a smart card as a proxy to the CA, such that each OBU has its own proxy. The proxy is equipped with a PIN system where a PIN is requested on power up, increasing proxy security. Theft of an OBU and malicious use are grounds for blacklisting an OBU. The main CA has a public-private key pair separate from the proxies; termed the CA‟s primary public-private key pair. All proxies have the same public-private key pair, which is referred to as the CA‟s secondary public-private key pair. The CA‟s primary and secondary public keys are known to all users.

The proxy needs to be able to provide an authentic certificate which contains the vehicle‟s permanent identity embedded in the certificate. The embedded vehicle‟s permanent identity needs to be incoherent information to other vehicles and readable by the main CA only. This ensures that no other node can retrieve the real identity of the vehicle, however if it is sent to the CA, the identity can easily be retrieved. There cannot however be any aspect of the proxy certificate that stays the same while pseudonyms change. As highlighted before, if the same permanent identity is embedded in each pseudonym certificate produced for a certain vehicle then there will be information that remains constant in the certificate even though pseudonyms change (solved in section 3.1.3). This creates a problem and means that the vehicle‟s permanent identity needs to be made to look different each time, without tampering with the true or permanent identity. The user must also not be able to create/modify a certificate or permanent identity; these certificates must therefore be „packed‟ and signed by the CA/CA‟s proxy. The proxy‟s signature in effect guarantees that the contents has not been altered and was created by the CA‟s proxy. It makes sense for the proxy to provide authentication for the vehicle. The development of the proxy certificate is discussed in the next section.

3.1 Proxy Certificate Development

The proxy certificate needs to incorporate authentication, privacy and traceability. Authentication must be provided by some trusted entity, which in this case can either be the main CA or proxy. The proxy is always on board the vehicle and is able to produce pseudonyms irrespective of availability of the main CA. Since the proxy has the same level of authority as the CA the pseudonym authentication should be provided by the proxy itself. The proxy can provide authentication in terms of a certificate. The authentication is

therefore provided by the proxy as a trusted certificate, which allows other vehicles to verify that the pseudonym is authentic and the vehicle is registered with the network.

As a recap, privacy functions to maintain that the real identity of a user cannot be determined and is best implemented in the form of a pseudonym [**64**]. The pseudonym needs to be contained in the certificate issued by the proxy in order for it to be certified. As explained in section 2.1, a pseudonym which has not been certified is merely a false name and has no authentication. Generally, certificates do not contain actual user identities but rather the public key corresponding to that identity. Each pseudonym requires a public-private key pair as messages sent by a vehicle have to be signed by the private key corresponding to a pseudonym. Since only the pseudonym‟s public key can be used to verify the signature, successful verification ensures that the authenticity of the message sent by the pseudonym can be verified. The pseudonym‟s public key therefore needs to be contained in the proxy‟s certificate and in effect certified by the proxy. The user‟s identity is provided by a permanent identity, which needs to be included in the certificate to enable tracing.

The proxy‟s certificate which combines authentication, privacy and traceability is shown in high level below:

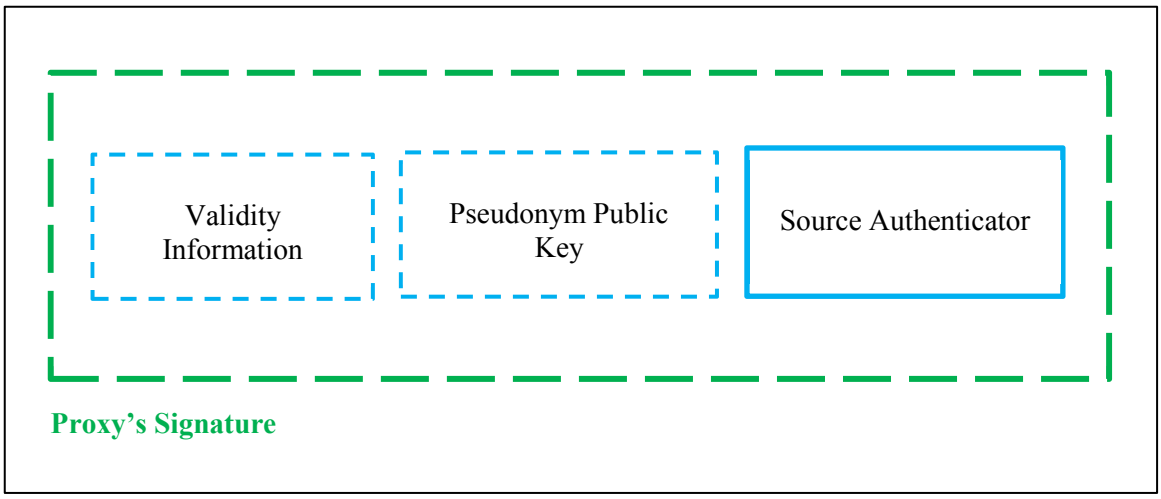

Figure 3-3 - High Level overview of Proxy's Certificate

The CA‟s proxy is the trusted entity which wraps this certificate (shown in green in the above diagram). Since all nodes know the CA‟s secondary public key, the signature on the proxy‟s certificate can easily be verified. The validity information and pseudonym public key remain in plaintext. The source authenticator needs to appear as unintelligible

information because it has to remain secret to preserve privacy. This is done by encrypting with the CA‟s primary public key.

It is essential for other nodes to know that the certificate is valid, the pseudonym is certified and the vehicle‟s real identity can be traced by the CA; these form the main aspects of the proxy‟s certificate. Each of these aspects is discussed further in their respective sections below.

3.1.1 Validity Information

The attributes needed to verify validity of the proxy‟s certificate are the Timestamp and Lifespan. The Timestamp indicates the time at which the proxy certificate was created and the Lifespan indicates the duration of the proxy certificate validity; these together act as an expiration date for the certificate [**92**].

It is essential to know if the proxy certificate contains valid information or not. This is because it has a major impact on the security of the system; if the certificate is not valid then it cannot be trusted as the information contained within might be expired or incorrect. A message might contain an invalid weather forecast or invalid information regarding traffic on roads, and if it is read and trusted a long time after the messages were sent it could result in unsafe routes been taken or trips postponed. Trusting expired or incorrect information can therefore be problematic. It is guaranteed that if the proxy‟s certificate can be unwrapped and the validity information indicates that the certificate is valid, then the information contained within the certificate is trusted and valid. The timestamp and lifespan can either be fields in a certificate or attached to a message. They effectively imply how long the validity of the authentication lasts or how long the message content is valid for.

3.1.2 Pseudonym Public Key

Kohlas and Maurer [**119**] state that an entity controls (or owns) the public key if it can use the corresponding private key to decrypt or sign data. One of the proxy‟s main responsibilities is to produce an authentic pseudonymous identity for the vehicle. Each time the proxy generates a pseudonym, a public-private key pair is also generated. The vehicle‟s pseudonym for a specific time is identified by the public key corresponding to that pseudonym. A transmitted message may be signed using the pseudonym‟s private key,

indicating that the message was produced by that pseudonymous identity. The pseudonym‟s public key is contained in the proxy‟s certificate as this is the key used to verify the authenticity of the signature on a transmitted message.

For the remainder of this chapter, the vehicle‟s pseudonym public-private key pair is denoted by (PU_V, PR_V), where PU_V is the pseudonym‟s public key and PR_V is the pseudonym‟s private key. PU_V is used to verify the signature made with PR_V on a message. PR_V is used to sign messages while communicating with other vehicles and to read messages that are intended for that particular pseudonym.

3.1.3 Certified Permanent Identity

The certified permanent identity functions mainly to provide traceability. As per the discussion on certification in section 2.1, it is evident that the vehicle‟s permanent identity should be a certified permanent identity (or permanent certificate). To ensure that the permanent certificate is kept secret, it needs to be a wrapped such that only authorized entities (in this case, the CA) can view the contents. This implies that the permanent certificate must be wrapped with the CA‟s primary public key, as only the main CA has the corresponding private key. To all vehicles, this identity appears as unintelligible information, therefore ensuring that the identity is kept secret.

The permanent certificate of the vehicle is fixed data and will not change over a long period of time, even though pseudonyms will be changing. While undergoing a traffic analysis attack, the same sequence of bits will be observed in each certificate sent from the vehicle. This is illustrated below:

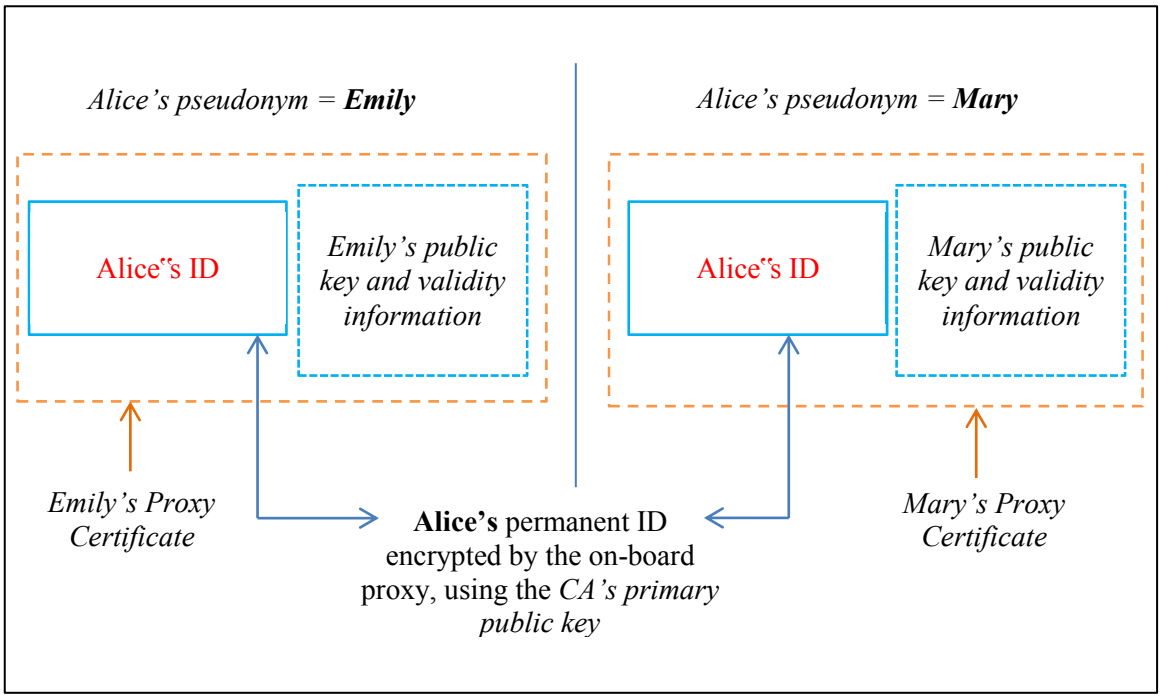

Figure 3-4 - Diagram illustrating constant identity information transmitted while pseudonym changes

From the diagram above it can be seen that even though Alice"s permanent identity is not readable by any node (as it is encrypted with the CA"s primary public key), it will contain the same sequence of bits for each pseudonym Alice uses. Even though Alice used pseudonyms Emily and Mary, which do not have any link to Alice, the static block containing Alice"s identity is present. This is where the vehicle"s privacy will be compromised. Therefore, to ensure privacy some sort of variation of the permanent certificate needs to be introduced. A timestamp could be used to make the message look different as could a nonce (random number). The use of a timestamp will provide information as to when the permanent identity was used for the current proxy certificate and so is preferred to the use of a nonce. Both the timestamp used to provide variation and the permanent certificate are wrapped to ensure that the information appears entirely different to any node in the network. A different timestamp will be used with each pseudonym as they would be produced at different times.

The vehicle"s permanent identity and timestamp for variation form the source authenticator and is implemented as follows:

$$Source\ Authenticator = E_{PU_{CA1}}(Permanent\ Certificate \,||\, Timestamp) \quad (1)$$

Where:

- $E_{PU_{CA1}}$ = Encryption with the CA's primary public key, PU_{CA1}
- $Permanent\ Certificate$ = The vehicle's permanent identity that has been certified by the CA
- $Timestamp$ = The time at which the encrypted block in equation (1) is created, functioning to add variation to the encrypted block.

The content wrapped in equation (1) above appears different each time the timestamp changes. Since each pseudonym is produced at a different instant in time, this ensures that the string of bits looks different for each pseudonym. Further, the wrapping with PU_{CA1} ensures that only the CA can view the content. This result of using a variable timestamp is illustrated below:

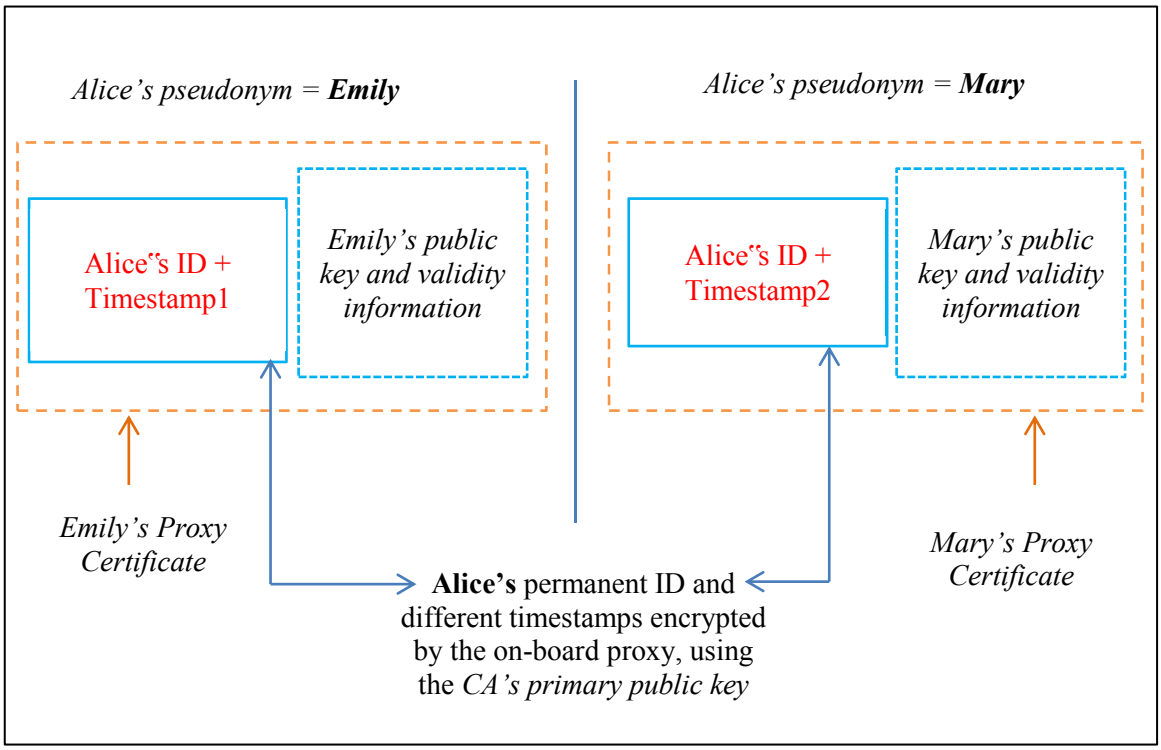

Figure 3-5 - Illustration of the effect of variable information on the permanent identity

The difference between figure 3-4 and figure 3-5 can clearly be seen. Since a different timestamp allows for the source authenticator block to look different each time, it is highly unlikely that two pseudonyms coming from the same source can be linked. Therefore, pseudonyms cannot be easily traced via their permanent identity. Emily‟s and Mary‟s certificates appear entirely different, due to the encrypted block of bits that are different, and do not appear to have any link to Alice.

Encryption with a public key could have been produced by any node as the CA‟s public keys are available to all nodes in the network. In order to maintain that the CA‟s proxy created the wrapping on the proxy certificate, the source authenticator (as defined in equation (1)) has to also be signed by the CA‟s proxy. If it is not signed by the CA‟s proxy then it cannot be considered valid or authentic because any node could have created an encrypted block of bits and wrapped it with the CA‟s primary public key. The proxy must therefore prove that it created the source authenticator. The proxy need not sign the source authenticator separately, as it is contained within the proxy‟s certificate (referring to figure 3-3). The proxy therefore ensures that the source authenticator is embedded in the proxy certificate, hence allowing for it to also have the proxy‟s signature.

The vehicle‟s permanent identity should be known and traceable by the main CA only. The main CA hands the vehicle‟s permanent certificate to the proxy upon registration. There is other essential information required to determine the validity of the permanent certificate: the timestamp and lifespan. In order to prove that only the main CA could have distributed this identity to the proxy, it is wrapped with the CA‟s primary private key. The certificate containing the vehicle‟s permanent identity which is handed to the proxy from the main CA looks as follows:

$$Permanent\ Certificate = E_{PR_{CA1}}(ID_V \ || \ Timestamp_{Permanent} \ || \ Lifespan_{Permanent}) \quad (2)$$

Where:

- $E_{PR_{CA1}}$ = Encryption with the CA‟s primary private key, PR_{CA1}
- ID_V = The vehicle‟s permanent identity
- $Timestamp_{Permanent}$ = Time that the permanent certificate was created
- $Lifespan_{Permanent}$ = Lifespan of the permanent certificate

The permanent certificate in equation (2) is used by the main CA to trace the source of the pseudonym. When a node behaves maliciously or is in distress and requires assistance, the CA attempts to trace a vehicle‟s identity. Upon verification of the main CA‟s signature, it is guaranteed that the permanent identity is indeed the one initially given to the proxy by the main CA. The validity information, i.e. the timestamp and lifespan, indicate if the certificate is valid. As per the reasons mentioned in section 3.1.1 the certificate cannot be trusted if it is not valid. The main CA holds a record of the permanent identity with other information about the vehicle; for example contact details for the vehicle‟s driver, date that the user registered with the network, a record if it has behaved maliciously before, etc. When a user is traced the CA is able to access all information maintained in the vehicle‟s record.

The resultant proxy certificate created to certify pseudonyms, while also embedding the source authenticator that can be viewed by the CA only can now be fully constructed. It is a combination of the source authenticator, the proxy certificate‟s validity information and pseudonym public key. These are the aspects that are represented in the high level breakdown of the proxy certificate in figure 3-3. Equation (1) provides the source authenticator, which allows only the CA to view the real identity of the vehicle. The validity information and pseudonym public key is necessary for validation and verification of the pseudonym‟s message, as explained in sections 3.1.1 and 3.1.2 respectively. The proxy certificate is therefore as follows:

$$Proxy\ Certificate = E_{PR_{CA2}}(Validity_{Proxy} \,||\, PU_V \,||\, (Source\ Authenticator)) \qquad (3)$$

Where:

- $E_{PR_{CA2}}$ = Encryption with the CA‟s secondary private key, PR_{CA2}
- $Validity_{Proxy}$ = The validity information for the proxy certificate. It is made up of $Timestamp_{Proxy}$ and $Lifespan_{Proxy}$ which are the time that the proxy‟s certificate was created and the lifespan of the proxy‟s certificate respectively.
- PU_V = The pseudonym public key
- $Source\ Authenticator$ = The combination of the vehicle‟s permanent identity and timestamp for variation. This is defined in equation (1).

As can be seen from equation (3), this proxy‟s certificate contains validity information, the pseudonym‟s public key and a block of information which can be viewed by the CA only,

containing the permanent identity of the vehicle. This thus caters for privacy and authentication, which also incorporates traceability. Authentication is provided by the proxy‟s signature, privacy is provided by the pseudonym and traceability is provided by the source authenticator. It is assumed that no other node is able to pose as the CA. The following diagram shows what Alice‟s proxy certificate looks like before transmission and how Bob unpacks Alice‟s proxy certificate:

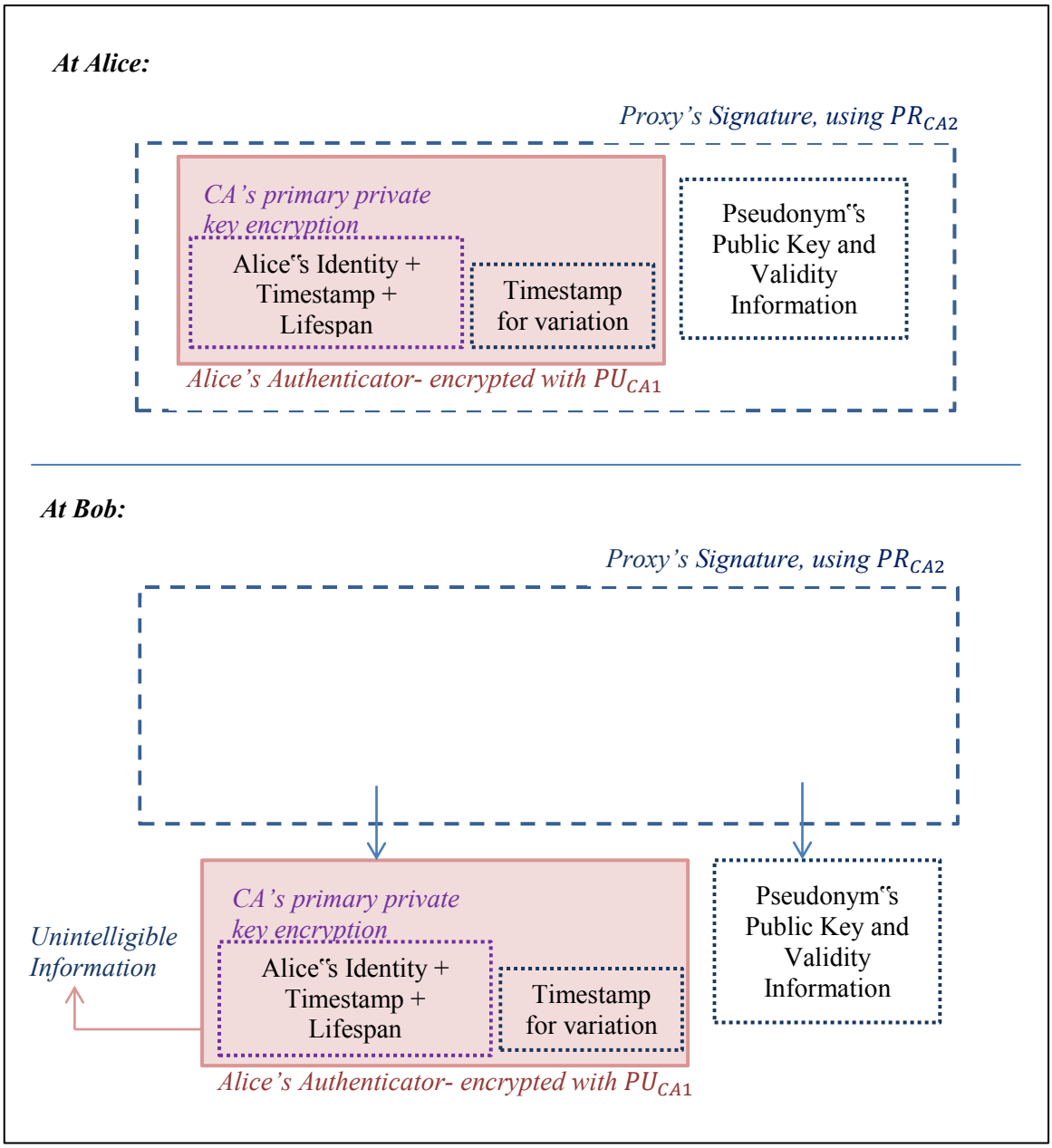

Figure 3-6 – Illustration of the packing, transmission and unpacking of the Proxy's Certificate

As can be seen in the figure above, Alice‟s proxy initially wraps her source authenticator and the pseudonym information (pseudonym public key, lifetime and timestamp) with the CA‟s secondary private key. This is transmitted, as the proxy‟s certificate. At Bob‟s node, the CA‟s secondary public key is used to verify the signature and upon verification Bob has access to the pseudonym information (pseudonym public key, lifetime and timestamp) and Alice‟s source authenticator. The source authenticator appears as unintelligible information.

3.2 Message Transmission

Due to the nature of VANETS most messages will be broadcast to many nodes. This means that messages do not need to always be encrypted because confidentiality is not necessary. This is because when a broadcast message is sent the message can be viewed by any user and therefore only message integrity and authentication are of concern; the pseudonym‟s signature therefore needs to appear on the message. If Alice wished to send a broadcast message under the pseudonym of Carol, the message would be signed by Carol and not encrypted in any way. The pseudonym‟s signature on the message is essential so that Carol can be authenticated. It is also essential to include an indication of when the message was sent so that the validity of the message can be determined. The transmitted message for a general broadcast scenario is shown below:

$$Transmitted\ Message = (Proxy's\ certificate) || E_{PR_V}(message\ ||\ timestamp_M) \quad (4)$$

Where:

- $Proxy's\ Certificate$ = defined in equation (3) above
- E_{PR_V} = Encryption with Carol‟s private key, PR_V
- $message$ = the message that has been sent, in plaintext
- $timestamp_M$ = the time that the message was created

The $message$ field in the above transmitted message is sent only with the pseudonym‟s signature and no wrapping to ensure confidentiality because it is a broadcast message; this implies that any node can see the contents of the message and confidentiality is not required. The pseudonym‟s certificate is carried with the message to enable other nodes to verify that the sender is authentic. The public key to verify the signature is contained in the proxy‟s certificate.

If one signs the message by encrypting the entire message, it is expensive to do at the sender. All receivers will need to unpack the certificate and then decrypt the whole message before they can read it. It would be wiser to merely sign a hash of the message (which is a shortened form of the message, calculated using some hash function [**112**]) and send it. A hash is commonly used to verify the integrity of a message. The resultant hash is signed (shown below was „signed hash") and sent together with the message to the recipient:

$$Signed\ hash = E_{PR_V}\left(h\ (message)\right) \quad (5)$$

Where:

- E_{PR_V} = Encryption with pseudonym private key, PR_V
- h = the hash function
- $message$ = the message in plaintext

The recipient verifies the signature on the signed hash and calculates the hash of the received message. If the signed hash matches with the calculated hash then the message is considered authentic and to have not been altered.

When compared to dividing the entire message into blocks and signing individually, this saves computation time and space [**112**]. There is therefore less work at the sender and every receiver is able to read the message directly and need only check certification. Many messages may never need to be checked as they will be self-evident quite shortly after reception and not dangerous or prone to malic.

In another scenario, if a Carol needs to send a message specifically to Dale (Bob"s pseudonym) the message must be encrypted with Dale"s public key, so that only Dale can unwrap it. The message hash and timestamp should thereafter be signed with Carol"s private key to confirm Carol created the message and that it is valid. Confidentiality of the message is required here because the message is meant for only Dale, and it is undesirable for other nodes to view it. This structure of the transmitted message is shown below:

$$Transmitted\ Message = (Proxy's\ certificate) || E_{PR_{V_C}}(h\ (message)\ ||\ timestamp_M\ ) || E_{PU_{V_D}}(message) \quad (6)$$

Where:

- $Proxy's\ Certificate$ = defined in equation (3) above
- $E_{PR_{V_C}}$ = Encryption with Carol‟s private key, PR_{V_C}
- $h\ (message)$ = Hash of the message
- $message$ = the message that has been sent, in plaintext
- $timestamp_M$ = the time that the message was created
- $E_{PU_{V_D}}$ = Encryption with Dale‟s public key, PU_{V_D}

As in the broadcast case, the proxy‟s certificate can be easily verified. The message hash and timestamp is signed by Carol and can be verified upon applying Carol‟s public key. The message has been wrapped using Dale‟s public key and this ensures that only Dale can unwrap the message, guaranteeing confidentiality. Confirming that the message hash signed by Carol matches a message hash calculated by Dale proves that the message is from Carol. Further, being able to verify the signature made with PR_{V_C} confirms that the message was produced by Carol (who is registered in the network and who can be traced to Alice by the CA if needed); guaranteeing integrity and authentication. If the message hash was altered after Carol signed it, it will no longer carry Carol‟s signature and will not be authentic or carry integrity.

3.2.1 Protocol Transaction

Transactions using the proposed protocol and demonstration of its effectiveness in achieving authentication and privacy are provided in this section.

Considering the scenario where a message from Carol is broadcast to other nodes and Dale chooses to reply to Carol, the following transactions will take place:

The OBU generates Alice‟s pseudonym (Carol) and a public-private key pair for Carol (PU_{V_C}, PR_{V_C}). The proxy thereafter creates an authenticator for Alice; a timestamp is combined with Alice‟s permanent certificate and both are encrypted using the CA‟s primary public key, as shown below:

$$Alice's\ Authenticator = E_{PU_{CA1}}(Alice's\ Permanent\ Certificate\ ||\ Timestamp) \quad (7)$$

The proxy generates validity information ($Validity_{Proxy}$) for the proxy certificate. This is made up of $Timestamp_{Proxy}$ and $Lifespan_{Proxy}$. The CA‟s secondary private key is used

to produce Carol‟s certificate by wrapping $Validity_{Proxy}$, Carol‟s public key (PU_{V_C}) and Alice‟s Authenticator:

$$Carol's\ Certificate = E_{PR_{CA2}}\ (Validity_{Proxy} \,||\, PU_{V_C} \,||\, Alice's\ Authenticator) \quad (8)$$

Carol‟s certificate follows the same structure as the proxy certificate defined in equation (3). The message hash is calculated, combined with the message timestamp and signed with PR_{V_C} to produce Carol‟s message signature:

$$Carol's\ message\ signature = E_{PR_{V_C}}(h\ (message) || timestamp_M) \quad (9)$$

Carol‟s certificate, message signature and original message are combined and transmitted:

$$Transmitted\ Message = (Carol's\ certificate) \,||\, Carol's\ message\ signature \,||\, message \quad (10)$$

This transmitted message is broadcast to each node in the area. Since all nodes have access to PU_{CA2} Carol‟s certificate can be verified.

Upon receiving the transited message, Bob does the following:

Bob uses PU_{CA2} to verify the signature on Carol‟s certificate. Upon verification, Bob can see the following:

$$D_{PU_{CA2}}(Carol's\ certificate) = Validity_{Proxy} \,||\, PU_{V_C} \,||\, (Alice's\ Authenticator) \quad (11)$$

Where:

- $D_{PU_{CA2}}$ = Performing a decryption or „unwrapping“ operation (in this case verifying the proxy‟s signature), using PU_{CA2}

Only $Validity_{Proxy}$ and PU_{V_C} can be read by Bob. Bob verifies that Carol‟s certificate is still valid using $Validity_{Proxy}$. If Carol‟s certificate is valid, PU_{V_C} is considered authentic and valid and is used to verify the signature on Carol‟s message signature:

$$D_{PU_{V_C}}(Carol's\ message\ signature) = h\ (message) || timestamp_M \quad (12)$$

Bob can then read Carol‟s message signature and view the message timestamp. If the message timestamp proves that the message was created within the valid time period, then the message is valid. He calculates the hash of the message, which has been sent in plaintext and if it matches the hash signed by Carol then it is certain Carol sent the message.

Thereafter assume Bob wants to respond to Carol regarding the broadcast message.

Bob‟s OBU generates a public private key pair for Dale (PU_{V_D} , PR_{V_D}). The proxy creates a certificate for Dale by combining a timestamp with Bob‟s permanent certificate and encrypting it using the CA‟s primary public key, as shown below:

$$Bob's\ Authenticator = E_{PU_{CA1}}(Bob's\ Permanent\ Certificate \,||\, Timestamp) \quad (13)$$

The proxy generates validity information ($Validity_{Proxy}$) for Dale‟s certificate. This is made up of $Timestamp_{Proxy}$ and $Lifespan_{Proxy}$. The CA‟s secondary private key is then applied to $Validity_{Proxy}$, Dale‟s public key (PU_{V_D}) and Bob‟s Authenticator to produce a certificate for Dale:

$$Dale's\ Certificate = E_{PR_{CA2}}\ (Validity_{Proxy} \,||\, PU_{V_D} \,||\, Bob's\ Authenticator) \quad (14)$$

Dale wraps the message such that it is visible to Carol only:

$$Encrypted\ message = E_{PU_{V_C}}(message\ ) \quad (15)$$

A hash of the message is then calculated. The message hash and a message timestamp are signed by Dale, producing Dale's message signature:

$$Dale's\ message\ signature = E_{PR_{V_D}}(h\ (message) || \ timestamp_M) \quad (16)$$

This result is combined with Dale‟s certificate and the encrypted message and transmitted:

$$Transmitted\ Message = (Dale's\ certificate) \,||\, Dale's\ message\ signature \,||\, Encrypted\ message \quad (17)$$

The message is thereafter sent to Carol; the outcome is shown below:

Carol verifies Dale‟s certificate and can see the following:

$$D_{PK_{CA2}}(Dale's\ certificate)$$
$$= Validity_{Proxy} \,||\, PU_{V_D} \,||\, (Bob's\ Authenticator) \quad (18)$$

Only $Validity_{Proxy}$ and PU_{V_D} can be read by Carol. Carol verifies that Dale‟s certificate is still valid using $Validity_{Proxy}$. If Dale‟s certificate is valid, PU_{V_D} is considered authentic and valid, and can be used as follows:

$$D_{PU_{V_D}}(Dale's\ message\ signature) = h\,(message) \,||\, timestamp_M \quad (19)$$

The message wrapped with PU_{V_C} can then be easily unwrapped by Carol using PR_{V_C}. The message hash is calculated, and as before, if both hashes match then the message did indeed come from Dale. This guarantees confidentiality and authentication.

The steps above demonstrate that the protocol caters for both authentication and privacy. Since the proxy is always available, this guarantees that authentic certificates are also always available. All proxies are considered trusted and are able to provide authentic pseudonyms that protect the user‟s real identity, while also ensuring that the CA can trace the vehicle if necessary.

Looking at the sequence of events above, this solution still keeps the PKI structure intact; there is a TTP (the CA), and nodes only accept certificates signed by the CA (a proxy to the CA in this case, which is trusted). Even though each node creates and signs their own certificates, this is not a distributed authority network, but rather one with a TTP, which ensures that the network is trusted.

3.3 Protocol Analysis

3.3.1 Proposed Solution Summary and Discussion

With reference to the proxy‟s certificate in equation (3), since the CA‟s secondary public key, PU_{CA2} is known to each node, the signature on the proxy‟s certificate can be easily verified. A signature using PR_{CA2} confirms that only the CA‟s proxy, a trusted entity, could have created the certificate. Once the certificate has been verified the fields for $Timestamp_{Proxy}$, $Lifespan_{Proxy}$ and PU_V appear in plaintext to the user. The source authenticator can only be seen by the CA, as it is wrapped with the CA‟s primary public key, guaranteeing confidentiality of the permanent identity. Upon verification of the

validity of the certificate the vehicle‟s pseudonym public key, $PU_{V,}$ is considered certified. This implies that the vehicle is registered with the CA and the CA can trace the vehicle‟s real identity; thus guaranteeing the vehicle is authentic and traceable.

The attributes of the proxy‟s certificate to ensure that the pseudonym is valid is the validity information: Timestamp and Lifespan. These are essential in determining if the certificate can be trusted or not; because even though the CA‟s secondary public key opens the proxy‟s certificate, it cannot be fully trusted unless it is valid. Certifying the pseudonym public key is the primary reason for the proxy‟s certificate. The pseudonym‟s public-private key pair is essentially the link to identifying the pseudonym. The public key is indicated in the proxy certificate to ensure that the signature on a message sent for the pseudonym can be verified with the proxy certified public key.

Other nodes will be able to verify that the proxy‟s certificate was created by the proxy as the CA‟s secondary public key is available to any node, but will not be able to read the contents of the information wrapped with the CA‟s primary public key. No node will be able to replicate the signature or alter the certificate contents after it has been signed with the CA‟s secondary private key because only the trusted proxy could have produced it. If the certificate is altered in any way, it will no longer carry the proxy‟s signature and will be considered invalid.

The smart card is ideal for implementing a proxy to the CA because of the convenience and reliability that it offers. The smart card is also able to perform complex cryptographic computations making it suitable for producing a certified pseudonym. It is tamper-proof; a security measure is that it will become useless if it is tampered with. There are also methods for implementing further security for the smart card; PIN codes and duress codes as mentioned at the start of this chapter. Since the smart card is embedded in the OBU, it is always available to the vehicle and can produce certified pseudonyms as and when needed. The smart card therefore provides a secure and convenient method for implementing the proxy, which functions mainly to produce a certificate for each pseudonym.

According to Hubaux et al. [**12**], an anonymity metric can be based on entropy. The entropy, in terms of information theory is defined by Dok et al. [**85**] as a measure of the content of a message evaluated with respect to its probability of occurrence, or uncertainty of occurrences. An attack on privacy in a VANET is where the attacker wants to retrieve a vehicle‟s identity by analysing identification messages that the victim transmits [**12**]. In

this system the permanent identification information is given by the source authenticator (indicated in equation (1) in section 3.1.3). For this system, it is not possible to determine the vehicle‟s real identity, as it is encrypted with the CA‟s primary public key, and can therefore only be unwrapped by the main CA. Further, the source authenticator appears different each time because a timestamp is combined with the permanent identity before encrypting with the CA‟s primary public key, thereby adding variation. It is therefore impossible to determine which vehicle a message has come from and the probability of finding an identity after attack is therefore nil. The degree of anonymity is directly dependent on the probability of finding an identity [**12**], and is therefore also nil for each pseudonym. This means that no information is given out for a pseudonym, and the system therefore guarantees privacy. In essence, since the anonymity cannot be tracked, the sender will remain anonymous.

A comparison of the success ratio between the scenario where the CA generates and distributes the certified pseudonyms, which is the most commonly used scheme in this field (examples are given in section 2.2.3) and the proposed solution shows that this proposed solution has the potential to perform well in South African networks. South African statistics [120] show that the 3G coverage is 81% for urban areas 12.9% for rural areas. When the CA generates and distributes certified pseudonyms, online access to the CA (i.e. 3G communications) is required to receive certified pseudonyms. Assuming that the vehicle is moving in all parts of the urban or rural area, while requesting a total of 100 certificates and is equally likely to request for a certificate in any part of the urban or rural area, then the success ratios may be approximated to be:

$$Urban\ area\ success\ ratio \simeq \frac{\frac{81}{100} x\ 100}{100} = 0.810 \qquad (20)$$

$$Rural\ area\ success\ ratio \simeq \frac{\frac{12.9}{100} x\ 100}{100} = 0.129 \qquad (21)$$

This shows that the CA is able to generate and distribute certified pseudonyms with a fairly high success ratio in urban areas and a low success ratio in rural areas. However, it is very likely that short distance trips in an urban area may always have 3G coverage; here, a success ratio greater than 0.810 is expected. The proposed solution does not possess this difference in success ratio in urban and rural areas, due to the fact that a certified pseudonym may be generated irrespective of online access to the CA. There is always a successful certification request for as long as the node is not declared as malicious. The

success ratio for above scenario of requesting 100 certificates is thus approximated to be close to 1:

$$Success\ ratio = \frac{\sim 100}{100} \simeq 1 \qquad (22)$$

This ratio is valid in both urban and rural areas. There is however the downside that the probability of a misbehaving node being undetected is high when the node is passive (i.e. not communicating with other nodes). During this case the joint detection probability (i.e. the probability of detecting an innocent node as misbehaving and the probability of misdetection of a malicious node), which gives an indication of the detection inaccuracy [**53**], is high:

$$Joint\ detection\ probability = 1 - \prod_{i=1}^{k}(1 - P_i') \simeq 1 \qquad (23)$$

Where:

P_i' = probability that a misbehaving node is undetected

k = number of nodes in the network

Since P_i' is large, the overall detection inaccuracy is high. This shows that even though the solution caters well for providing a certified pseudonym when the CA is not present, it cannot guarantee that a malicious node will not exist. The malicious node will be able to exist for a long while in a passive mode; the negative effect is that it is able to eavesdrop on the network traffic. This is not detrimental to the network because the messages that need to be kept secret are encrypted. If the node becomes active and decides to flood the network with inconsistent or redundant information then it will be identified as the network is monitored for inconsistent spikes in network traffic.

The initial overhead involved in this proposed scheme is greater than those analysed in sections 2.2.1 – 2.2.3 because each vehicle needs to be equipped with an OBU. In the long run, the overhead is less than that where the node produces pseudonyms and sends to the CA for certification because connections to the CA are not necessary for generating certified pseudonyms.

There are attacks that may occur on this system in order to compromise the privacy. Replay attacks are one such attack; this enables malicious nodes to cause confusion in the network.

Vehicles may also attempt to cheat and create false certified pseudonyms. The solution is discussed in terms of how it will handle these attacks in the section below.

3.3.2 Possible Attacks

This section details some attacks that could affect the solution and how it would cope in each instance:

A malicious node could want to alter a proxy‟s certificate and attach it to a false message, so that it is traced to some other vehicle. This will not be possible here because once the proxy‟s certificate is altered it will not carry a trusted signature and will therefore not be valid. A node could also try to create a false proxy certificate and pretend it is registered with the CA. In this situation, the malicious node will not have access to the CA‟s secondary private key and cannot create trusted proxy certificates. The malicious vehicle therefore has no means of sending messages with a certified pseudonym. A false certificate may be created but it will not be trusted as it does not have the proxy‟s signature.

Replay attacks, where a message is played at a later time, may occur. This type of attack will cause confusion in the network as messages that may not be valid will be circulated. VANET messages generally have short lifespans because the network is dynamic in nature and a certain warning may not be of concern at a later time. Therefore, the replayed message would not be valid and would be discarded. It can however cause flooding of the network when too many messages are replayed.

Malicious nodes could try to attack the protocol (jeopardize the security) given above, either by trying to falsely join the network or by becoming malicious once part of the network. Due to the existence of the CA, it will not be possible for a malicious node to register with the network. This is because all messages are only considered valid when accompanied by a certificate signed by the CA‟s proxy. A node that has not been registered with the network will not have an OBU with the CA‟s proxy; hence no proxy certificates will be created. The proxy is also built into the OBU and once physically damaged is rendered useless. Tampering with or stealing another vehicle‟s OBU is made difficult with blacklisting, PIN codes and duress codes, as mentioned at the beginning of this chapter.

When a node starts performing malicious acts after being registered with the network, the CA eventually finds out; there could be many users reporting false messages sent by certain pseudonyms, which when checked have the same permanent identity or irregularities in the

network traffic could be noticed. The malicious node becomes blacklisted and the proxy associated with that vehicle is no longer able to produce pseudonyms/certificates. The CA is able to trace the vehicle‟s permanent identity (using the permanent certificate). This is also discussed at the start of this chapter. Once the OBU has been blacklisted and the vehicle is deregistered, authentic messages may no longer be sent. If Alice has been blacklisted, it is therefore not possible that Bob will believe a message came from Alice as there will be no proxy certificate accompanying Alice‟s message.

Altering/forging certificates and behaving maliciously are catered for with the solution. The proxy‟s certificate which contains variable information to make the source authenticator appear different for each pseudonym is a major contribution to aiding with privacy and ensuring that no patterns between the vehicle‟s current and previous pseudonyms may be developed. Another important contribution to ward off attacks is the security provided by the smart card as the confidential information and algorithms stored on the card are well protected. Using the on board proxy to produce certified pseudonyms is how the problem of producing pseudonyms in the absence of the CA, that are authentic and traceable by the CA only can be addressed.

4. Conclusion

In recent times, MANETs have gained much exposure. The importance of MANETs cannot be overlooked as the computing world is becoming more portable and compact. Their ease of use and convenience make them ideal for emergency type situations. The classification of MANETs considered in this research were VANETs. VANETs allow for communication between vehicles and promote safety on roads. As discussed in the dissertation, due to the mobile nature of the VANET nodes, the CA may be unavailable at times; implementing privacy and authentication is thus prone to difficulties.

The research focused on providing privacy in VANETs while ensuring vehicles are authentic and traceable by the CA. Privacy was described as necessary to prevent users from being traced or followed, and is implemented through pseudonyms. These are false names which function to mask the vehicle‟s permanent identity. The pseudonyms need to be authentic in order to be trusted, hence the requirement of authentication which is provided by certificates. Pseudonyms and certificates are generated via cryptographic means. Privacy (provided by pseudonyms) and authentication (provided by certificates) are conflicting tenets of security. The objective of the research was to determine if it is possible for a vehicle to produce pseudonyms for itself that would still carry the authority of the CA and would be traceable by the CA while remaining anonymous to all other nodes.

The dissertation started with a classification of networks and a description of Ad Hoc Networks and MANETs in Chapter 1. The applications and challenges of these networks were also presented. A detailed description of VANETs, their unique characteristics and security issues were thereafter discussed. Chapter 2 focused on the privacy aspects of VANETs. The concept of pseudonyms was detailed and followed by reasons for the need for privacy in a VANET. Possible attacks on the privacy aspect in VANETs were thereafter presented. A section on certification followed, and the use of certificates in providing authentication was discussed. The chapter thereafter presented a thorough discussion on four main pseudonym generation mechanisms found in the literature followed by three pseudonym reuse methods. The solution was detailed in chapter 3. At the beginning of chapter 3, the requirements were outlined and smart cards were introduced. Mechanisms used to meet the requirements were then discussed, followed by the solution development. Thereafter the solution was demonstrated in terms of protocol transactions. This was followed by an analysis of the solution; a summary and discussion was presented, and the chapter ended with ways in which the solution copes with certain attacks.

The solution made use of a proxy on board each vehicle to produce certified pseudonyms as and when needed, which copes well in the absence of the CA. This is because access to the CA is not needed to produce certified pseudonyms. The proxies are smart cards as they have remarkable abilities of performing cryptographic computations and keeping private information confidential. They have been used widely in the mobile phone industry and the global banking industry. Smart cards are damaged when tampered with, hence allowing for confidential information to remain private. The proxy mainly functions to produce certified pseudonyms. The proxy certificate functions to certify the pseudonym‟s public key and provides traceability by embedding in it the source authenticator. This source authenticator contains variable information ensuring that the proxy‟s certificate appears different for each pseudonym. This aids with privacy and is also a solution to the problem experienced in the modified pseudonymous authentication approach discussed in section 2.2.4.

The appendix provides details on smart cards; their classification and history is presented. Due to the success of these smart card systems they are proven to be reliable and are suitable for the implementation of a proxy to the CA.

4.1 Summary of Contributions

The main contribution of this dissertation is a novel approach for ensuring both authentication and privacy in VANETs, catering for when the CA is unavailable. The method also incorporates traceability. Another contribution is the detailed discussion on MANETs and VANETs, in terms of their architecture, applications and challenges. This provides a comprehensive literature review in which prominent researchers in the field are made reference to. There has also been a thorough description of the need for privacy in VANETs. The last contribution is a comprehensive survey and discussion on the pseudonym generation mechanisms in VANETs.

4.2 Future Work

The future work on this research is:

- Enhance and simulate the solution in a realistic mobility model.
- Analyse certificate revocation options and solutions.

5. Appendix

There are smart cards in use currently that contain non-volatile memory and microprocessor components which can fit into a mobile device (cellular phone or vehicle) [**111**]. These are remarkable devices that can perform complex cryptographic algorithms and store information, while being very secure [**111**]. These cards are made of plastic, generally polyvinyl chloride [**113**]. They are not self-powered and rely on power from a card reader. A classification of smart cards is presented below:

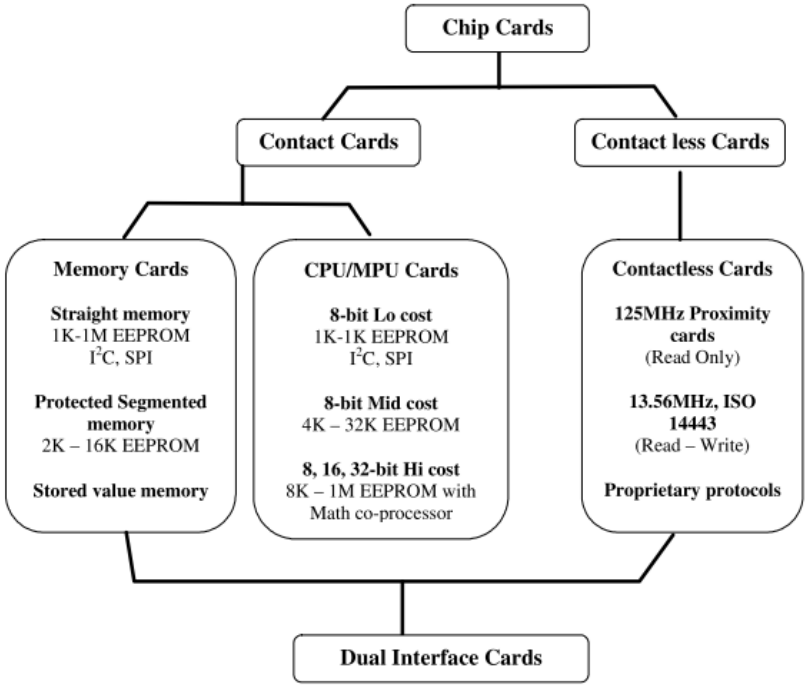

Figure A-1 - Classification of Smart Cards [112]

Memory cards are those that only store data; they are used in low cost applications and are not considered as their use is limited. Contactless smart cards make use of radio frequency technology between the smart card and a card reader. Their memory capacity is however significantly lower than that of contact smart cards. Contact smart cards are used in bank cards, credit cards and SIM cards for mobile telephones. According to Bhatt [**112**], SIM cards are the most commonly used type of smart card. They have a typical pin out, as shown below:

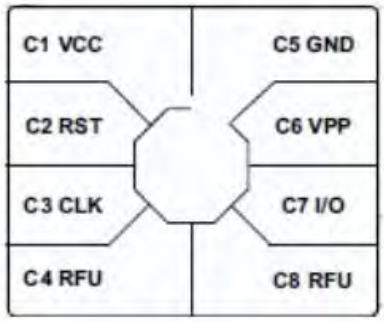

Figure A-2 - Contact Smart Card Pin Out [121]

The contact smart card operates when exposed to a card reader, which has the corresponding pin out shown above and powers the smart card. An application of this type of smart cards are those with data processing capabilities; a microprocessor within the card manages the memory allocation or file processing [**112**].

According to ChunXiao et al. [**116**], the smart cards breakthrough occurred in 1984 when French Postal and Telecommunications Services Authority performed a successful trial with smart cards in telephones. The smart cards met all expectations for high reliability and protection against manipulation. The following diagram illustrates the soar in productivity of smart cards in recent years:

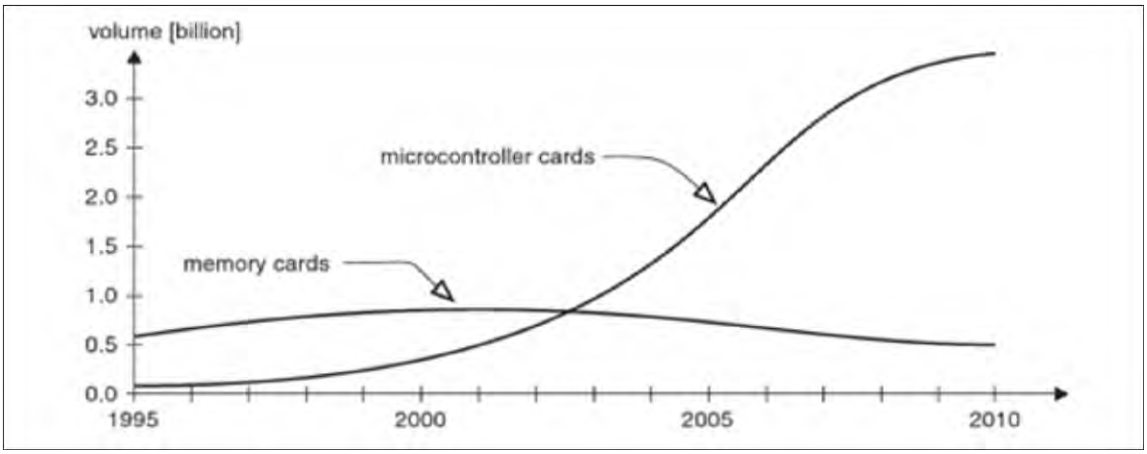

Figure A-3 - Estimated World Production Figures for Microcontroller Cards and Memory Cards [116]

With reference to Figure A-3, the microcontroller cards are the smart cards that can perform operations (for example cryptographic algorithms) and memory cards are those that do not have any computational ability and can only store data. It is noticed from the diagram that in recent years, there has been an exponential growth in the production of smart cards, implying that the demand has increased tremendously. Since memory cards do not have the ability to perform operations and their use is limited, the production has decreased. There has also been an increase in the amount of cellular phones (depicted in a graph produced by the Information Communications Union below) and this in effect has raised the smart card production; further indicating the reliability of smart cards. Czerniewicz [**122**] has drawn this conclusion and presents the following graph:

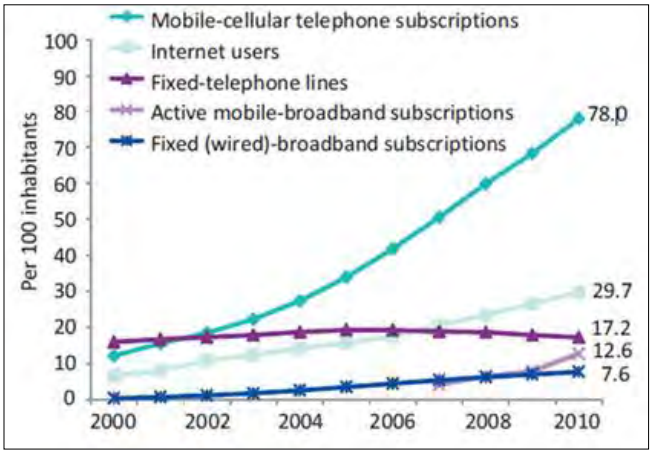

Figure A-4 - Comparison between number of people using Mobile Telephones, Internet, Fixed Telephone Lines, Mobile Broadband And Fixed Broadband Subscriptions [118]

There has been a sharp rise in mobile telephones users in recent years. As can also be seen from Figure A-4, the exponential increase in mobile telephone users correlates to an exponential increase in the amount of smart cards produced (Figure A-3). This can be attributed to the secure and convenient nature of these smart cards. Czerniewicz [**122**] claims that using the SIM (Subscriber Identity Module) card in a mobile telephone as a secure storage and computing module is how the mobile telephone has gained its trustworthiness.

Petri [**111**] states that the smart card is fairly resistant to being tampered with, as any physical damage will render the card useless.

In a study conducted by Datamonitor [**123**] , an information company specialising in industry analysis, there are a wealth of potential uses for smart cards. The United States smart card market value, which comprises only 4% of the global smart card market[**123**], rose by a massive 123% between 2000 and 2001 as shown below:

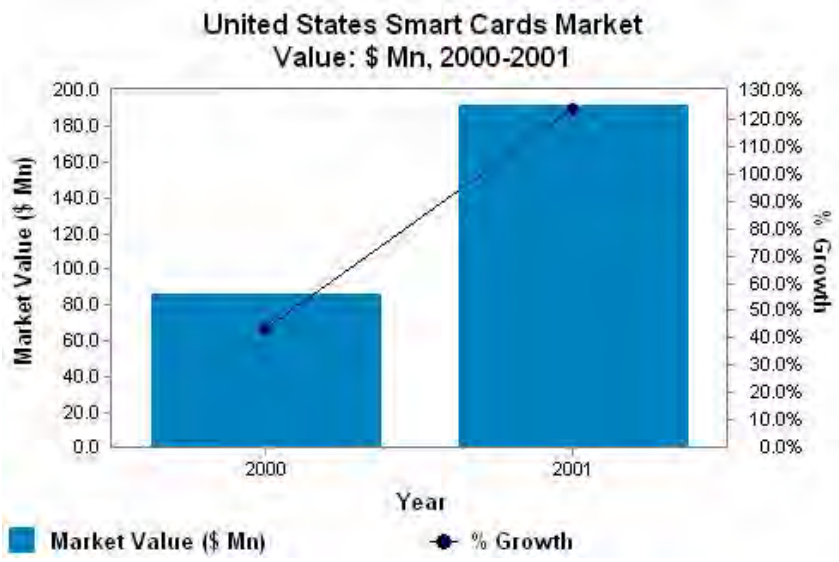

Figure A-5 - Rise in Smart Card Market Value in the United States [123]

This rise in smart card market value continues until this day, as smart cards are becoming more efficient and capable of performing larger, more complex algorithms.

Smart cards are small gadgets able to perform complex computations; this makes it apt for scenarios where authentication is required. Users also do not need to carry large documents as forms of identification as this can be done through a small smart card, offering convenience.

6. References

[1] Yang S.C, "Toward a Wireless World", *IEEE Technology and Society Magazine*, 2007, pp. 32 - 42

[2] Bhavnani A, Won-Wai Chiu R, Subramaniam J, and Silarszky P, "The role of mobile phones in sustainable rural poverty reduction", Global Information and Communications Department, ICT Policy Division 2008.

[3] Rao M, "Mobile Africa Report 2011", MobileMonday, 2011.

[4] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011–2016", United States of America, White Paper 2012. Retrieved March 21, 2012 (www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html)

[5] Bersin J, "Driving Organizational Performance amidst an Imbalanced Global Workforce 2011", Research Report. Retrieved February 12, 2012 (http://www.bersin.com/Practice/Detail.aspx?id=15034)

[6] Perkins C.E, "Ad Hoc Networking: An Introduction," Nokia Research Centre, 2000.

[7] McDanial P, La Porta T.F and Choi H, "Privacy Preserving Communication in MANETs,". Retrieved January 17, 2012 (http://www.cse.psu.edu/~tlp/paper/anon_secon.pdf)

[8] Sakib-Khan AP, Ed., *Security of Self Organising Networks: MANET, WSN, WMN, VANET*, 1st ed. Boca Raton: Auerbach Publications, 2011.

[9] Boukerche A, *Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks* , 1st ed.: Wiley-IEEE Press , 2009.

[10] Nowey T, Mletzko C and Plobl K, "Towards a Security Architecture for Vehicular Ad Hoc Networks," in *Proceedings of the International Conference on Availability, Reliability and Security*, 2006, Washington, pp. 374 - 381.

[11] Many, *VANET Vehicular Applications and Inter-Networking Technologies*, 1st ed., Hannes Hartenstein and Kenneth P. Laberteaux, Eds. West Sussex, United Kingdom: John Wiley and

Sons Ltd, 2010.

[12] Hubaux J.P, Capkun S, and Luo J, "The Security and Privacy of Smart Vehicles," in *IEEE Computer Society Security and Privacy Magazine*, 2004, pp. 49 - 55.

[13] Das S, Security Issues in MANETs. Retrieved October 5, 2011 (www.cs.ucsb.edu/~sudipto/talks/Security.pps).

[14] Gunter Y and Großmann H.P, "Usage of Wireless LAN for Inter-Vehicle Communication," in *8th International IEEE Conference on Intelligent Transportation Systems*, Vienna, 2005, pp. 296 - 301.

[15] Wang Y, Yi Z, Tian D, and Xia H, "Safety Message Transmitting Method for Vehicle Infrastructure Integration," in *Advanced Forum on Transportation of China*, 2010, Beijing, pp. 240 - 246.

[16] Aboudagga N, Refaei M.T, and Eltoweissy M, "Authentication Protocols for Ad Hoc Networks: Taxonomy and Research Issues," in *ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks*, 2005, Montreal, pp. 96 - 104.

[17] Sehgal U, Kaur K, and Kumar P, "Security in Vehicular Ad-hoc Networks", in *International Conference on Computer and Electrical Engineering*, December 2009, Dubai, pp. 485 - 488.

[18] Kargl F et al., "Research Challenges in Intervehicular Communication: Lessons of the 2010 Dagstuhl Seminar*", IEEE Communications Magazine*, vol. 49, no. 5, 2011, pp. 158 - 164.

[19] Weerasinghe H, Fu H, and Leng S, "Enhancing Unlinkability in Vehicular Ad Hoc Networks", in *IEEE International Conference on Intelligence and Security Informatics* , 2011, pp. 161 - 166.

[20] Chim T.W, Yiu S.M, Hui L, and Li V, "Security and Privacy Issues for Inter-vehicle Communcations in VANETs", *in IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks,* 2009, pp. 1 - 3.

[21] Hekmat S, "Communication Networks", PragSoft Corporation, 2005. Retrieved December 13, 2011 (www.pragsoft.com/books/CommNetwork.pdf)

[22] Haykin S, *Communication Systems*, 4th ed., Bill Zobrist, Ed. United States of America: John Wiley and Sons, 2001.

[23] Zhu W, Reibman A.R, Lagendijk R.I, and Chen C.W, "Introduction to the Special Issue on Wireless Communication", *IEEE Transactions on Circuits and Systems for Video Technology*, June 2002, vol. 12, no. 6, pp. 357 - 359.

[24] Ma Y, Han J.J, and Trivedi K.S, "Composite Performance and Availability Analysis of Wireless Communication Networks", *IEEE Transactions n Vehicular Technology*, September 2001, vol. 50, no. 5, pp. 1216 - 1223.

[25] Choi S, Kim B.K, Park J, Kang C, and Eom D, "An Implementation of Wireless Sensor Network for Security System using Bluetooth", *IEEE Transactions on Consumer Electronics*, February 2004, vol. 50, no. 1, pp. 236 - 244.

[26] Mark G and Su N.M, "Making infrastructure visible for nomadic work", *Pervasive and Mobile Computing Journal*, 2010, pp. 1 - 12.

[27] Hoebeke J, Moerman I, Dhoedt B, and Demeester P, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Ghent University, Belgium, Department of Information Technology, pp. 60 - 66.

[28] Sun J, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing," University of Oulu, Finland. Retrieved March 14 , 2011 (http://www.mediateam.oulu.fi/publications/pdf/92.pdf.).

[29] Keshav S, "Why Cell Phones Will Dominate the Future Internet", School of Computer Science, University of Waterloo, Canada. Retrieved February 16, 2012 (http://www.cl.cam.ac.uk/research/srg/netos/sla/mobileman/related/cellphonev3.pdf).

[30] Leung L and Wei R, "More than just talk on the move: Uses and gratifications of the cellular phone", *Journalism and Mass Communication Quarterly*, 2000, vol. 77, no. 2, pp. 308 - 320.

[31] Farely T and Schmidt K, "Cellular Telephone Basics", Private Line Telecommunications Expertise, 2006. Retrieved September 15, 2011 (http://www.privateline.com/mt_cellbasics/).

[32] Banks K and Burge R, *Mobile Phones: An appropriate tool for consrervation and development?*, 1st ed. Cambridge, United Kingdom: Fauna & Flora International, 2004.

[33] Goldsmith A, *Wireless Communications*, 1st ed. United States of America: Cambridge University Press, 2005.

[34] Khayat M.M, "Wireless Local Area Network (WLAN): Advantages vs. Disadvantages", Professional Seminar INNS 690, 2002.

[35] Zhou L and Haas Z.J, "Securing Ad Hoc Networks," in *IEEE Special Issue on Network Security*, 1999 , vol. 13, no. 6, pp. 24 - 30.

[36] Chen W, Guha R.K, Kwon T.J, Lee J, and Hsu I.Y, "A Survey and Challenges in Routing and Data Dissemination in Vehicular Ad Hoc Networks", in *IEEE International Conference on Vehicular Electronics and Safety*, 2008, Columbus, pp. 328 - 333.

[37] Gomez J and Garcia-Macias J.A, "MANET and WSN: Are they alike?", National University of Mexico, Coyoacan, 2006.

[38] Weiser M, "Some computer science issues in Ubiquitous Computing", *Communications of the ACM*, July 1993, vol. 36, no. 7, pp. 75 - 83.

[39] Mamatha G.S and Sharma S.C, "Analyzing the MANET variations, challenges, capacity and protocol issues", *International Journal of Computer Science & Engineering Survey (IJCSES)*, August 2010, vol. 1, no. 1, pp. 14 - 21.

[40] Choi H, McDanial P, and La Porta T.F, "Privacy Preserving Communication in MANETs", The Pennsylvania State University, Networking and Security Research Center. Retrieved August 14, 2011 (w.cse.psu.edu/~tlp/paper/anon_secon.pdf).

[41] Sakib R.K, "Security Issues in VANET", BRAC University, Bangladesh, 2010.

[42] Azer M.A, "Security in Ad Hoc Networks, from vulnerability to risk management", in *International Conference on Emerging Security Information, Systems and Technologies*, 2009, Cairo, pp. 203 - 209.

[43] Barker W.C, "Guideline for Identifying an Information System as a National Security System", National Institute of Standards and Technology, Gaithersburg, NIST Special Publication MD 20899-8930, 2003.

[44] Blumenthal M, "Encryption: Strengths and Weaknesses of Public-Key Cryptography",

Villanova University, Villanova, Computing Research Topics CSC 3990, 2007.

[45] Li Z, Xu Z, Yang J and Zhang W, "A New Certificateless Threshold Signature Scheme for Mobile Ad Hoc Network", in *Computer and Communication Technologies in Agriculture Engineering*, 2010, pp. 338 - 342.

[46] Buttya L, Hubaux J.P and Capkun S, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, January- March 2003, vol. 2, no. 1, pp. 52-64.

[47] Capan M, "Self-organizing software agents for communication management in Mobile Ad Hoc Networks", in *International Conference on Information and Communication Technology, Electronics and Microelectronics*, 2010, Croatia, pp. 485 - 490.

[48] Artimy M.M, Robertson W, and Phillips W.J, *Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks*, 1st ed., Azzedine Boukerche, Ed.: John Wiley & Sons, 2009.

[49] CREN and DLF, "Digital Certificate Infrastructure", Washington, 2002. Retrieved June 25, 2011 (www.cren.net/crenca/docs/cren-dlf.pdf)

[50] Kapidzic A.D.N, "A Certificate Management System: Structure, Functions and Protocols", in *Proceedings of the Symposium on Network and Distributed System Security*, 1995, San Diego, pp. 153 - 160.

[51] Yi S and Kravets R, "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks", *Proceedings of the 2nd Annual PKI Research Workshop*, 2003.

[52] Schneider F.B, Renesse R.V and Zhou L, "COCA: A Secure Distributed Online Certification Authority", *ACM Transactions on Computer Systems*, November 2002, vol. 20, no. 4, pp. 329–368.

[53] Lu S, Zerfos P, Kong J, and Luo H, "URSA: Ubiquitous and Robust Access Control for Mobile Ad-Hoc Networks", in *IEEE/ACM Transactions on Networking*, 2004, vol. 12, no. 6, pp. 1049 - 1063.

[54] Hubaux J.P, Eugster P.T and Luo J, "DICTATE: DIstributed CerTification Authority with probabilisTic frEshness for Ad Hoc Networks", *IEEE Transactions on Dependable and Secure Computing*, October - December 2005, vol. 2, no. 4, pp. 311 - 323.

[55] Padmadas M, Nallaperumal K, Mualidharan V, and Ravikumar P, "A deployable architecture of Intelligent Transportation System - A developing country perspective", in *IEEE International Conference on Computational Intelligence and Computing Research*, 2010, Podhigai, pp. 1 - 6.

[56] Harri J, Filali F, and Bonnet C, "Mobility Models for Vehicular Ad Hoc Networks: A Survey and Taxonomy", *IEEE Communications Surveys and Tutorials*, 2009, vol. 11, no. 4, pp. 19 - 41.

[57] Papadimitratos P et al., "Secure Vehicular Communication Systems: Design and Architecture", *IEEE Communications Magazine: Topics in Automotive Networking*, November 2008, pp. 100 - 114.

[58] Sumra I.A, Hasbullah H, Ahmad I, and Manan J.L, "Forming Vehicular Web of Trust in VANET", in *Saudi International Electronics, Communications and Photonics Conference*, 2011, Tronoh, pp. 1 - 6.

[59] IEEE, "IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications ", IEEE STD 802.11-1997, 1997.

[60] Worldometer, Real Time World Statistics, 2012. Retrieved January 21, 2012 (http://www.worldometers.info/cars/)

[61] Calandriello G, Papadimitratos P, Hubaux J.P, and Lioy A, "On the Performance of Secure Vehicular Communication Systems", *IEEE Transactions on Dependabe and Secure Computing*, November 2011, vol. 8, no. 6, pp. 898 - 912.

[62] Sterling B, "Turning cars into wireless network nodes", June 2007. Retrieved January 25, 2012 (http://www.wired.com/beyond_the_beyond/2007/06/turning_cars_in/).

[63] Fonseca E, Festag A, Baldessari R, and Aguiar R, "Support of Anonymity in VANETs – Putting Pseudonymity into Practice", in *IEEE Wireless Communications and Networking Conference*, Hong Kong, 2007, pp. 3400 - 3405.

[64] Festag A, Baldessari R and Zhang W, "Vehicular wireless short-range communication for improving intersection safety", in *IEEE Communications Magazine,* November 2009, vol. 47, no. 11, pp. 104 - 110.

[65] Papadimitratos P, Calandriello G, Hubaux J.P, and Lioy A, "Impact of Vehicular Communications Security on Transportation Safety", in *IEEE INFOCOM Workshop*, 2008, Laussane, pp. 1- 6.

[66] Blum J.J, Eskandarian A, and Hoffman L.J, "Challenges of Intervehicle Ad Hoc Networks", *IEEE Transactions on Intelligent Transportation Systems*, December 2004, vol. 5, no. 4, pp. 347 - 351.

[67] Kopitz D and Marks B, *RDS: The Radio Data System*, 1st ed. Boston, London: Artech House, 1999.

[68] Su W, Lee S.J, and Gerla M, "Mobility prediction in wireless networks", in *MILCOM: 21st Century Military Communications Conference* , 2000, pp. 491 - 495.

[69] Schaub F, Ma Z, and Kargl F, "Privacy Requirements in Vehicular Communication Systems", in *IEEE International Conference on Privacy, Security, Risk, and Trust* (PASSAT 2009), *Symposium on Secure Computing* (SecureCom09), 2009, Vancouver, pp. 139 - 145.

[70] Samara G, Al-Salihy W.A, and Sures R, "Security Analysis of Vehicular Ad Hoc Networks", in *Second International Conference on Network Applications, Protocols and Services*, 2010, pp. 55 - 60.

[71] De Fuentes M.D, González-Tablas A.I, and Ribagorda A, "Overview of security issues in Vehicular Ad-hoc Networks", in *Handbook of Research on Mobility and Computing,* 2011.

[72] Chaurasia B.K, Verma S, Tomar G.S, and Bhaskar S.M, "Pseudonym Based Mechanism for Sustaining Privacy in VANETs", in *International Conference on Computational Intelligence, Communication Systems and Networks*, 2009, pp. 420 - 425.

[73] Samara G, Al-Salihy W.A, and Sures R, "Security Issues and Challenges of Vehicular Ad Hoc Networks", in *International Conference on New Trends in Information Science and Service Science (NISS)*, 2010, pp. 393 - 398.

[74] Gerlach M, "Assessing and Improving Privacy in VANETs", in *Proceedings of Workshop on Embedded Security in Cars*, 2006.

[75] Kargl F, Wiedersheim B, Ma Z, and Papadimitratos P, "Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough", in *International Conference on Wireless On-*

demand Network Systems and Services, 2010, pp. 176 - 183.

[76] Kargl F et al., "Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges", in *IEEE Communications Magazine: Topics in Automotive Networking*, 2008, pp. 110 - 118.

[77] Many, *Vehicular Networking: Automotive Applications and Beyond*, 1st ed., M Emmelmann, B Bochow, and Kellum C C, Eds. Wiltshire, Great Britain: John Wiley and Sons, 2010.

[78] Lawson A, "Adopting a pseudonym can preserve privacy", Butler Group Review, 2003. Retrieved October 21, 2011 (www.sapior.com/Lawson_pseudonym_BGReview_Sep03.pdf).

[79] Gerlach M and Guttler F, "Privacy in VANETs using Changing Pseudonyms - Ideal and Real", in *IEEE Vehicular Technology Conference*, 2007, pp. 2521 - 2525.

[80] Beard C, "Pseudonyms", Indiana Standards, Web English Teacher 2004. Retrieved June 27, 2011 (www.webenglishteacher.com/msb/pseudonyms.pdf)

[81] Chaurasia K.B and Verma S, "Optimizing Pseudonym Updation for Anonymity in VANETs", in *IEEE Asia-Pacific Services Computing Conference*, 2008, pp. 1633 - 1637.

[82] Mahajan S and Jindal A, "Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks", *International Journal of Computer Applications*, February 2012, vol. 1, no. 20, pp. 17 - 21.

[83] Lu R, Lin X, and Luan T.H, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs", *IEEE Transactons on Vehicular Technology*, July 2011, vol. 61, no. 1, pp. 86 - 96.

[84] Sommer C, Ganseny T, German R and Eckhoff F.D, "Strong and Affordable Location Privacy in VANETs: Identity Diffusion Using Time-Slots and Swapping", in *IEEE Vehicular Networking Conference*, 2010, pp. 174 - 181.

[85] Dok H, Fu H, Echevarria R, and Weerasinghe H, "Privacy Issues of Vehicular Ad-Hoc Networks", *International Journal of Future Generation Communication and Networking*, March 2010, vol. 3, no. 1 , pp. 17 - 32.

[86] Mell P, Kent K, and Nusbaum J, "Guide to Malware Incident Prevention and Handling", NIST, Gaithersburg, Recommendations of the National Institute of Standards and Technology 800-83,

2005.

[87] Freudiger J, Hubaux J.P, and Meyer S, "Misbehavior in Mobile Application Markets", *Security and Cooperation in Wireless Networks Mini-project* 2010. Retrieved August 16, 2011 (www.arxiv.org/pdf/1107.1101).

[88] Papadimitratos P, Kung A, Hubaux J.P, and Kargl F, "Privacy and Identity Management for Vehicular Communication Systems: a Position Paper", IST-027795, *Workshop on Standards for Privacy in User-Centric Identity Management*, Zurich, 2006

[89] Diffie W and Hellman M.E, "Privacy and authentication: An introduction to Cryptography", *Proceedings of the IEEE Transactions in Cryptography and Security*, 1979, vol. 3, no. 67, pp. 397 - 427.

[90] Aziz M.I and Akbar S, "Introduction to Cryptography", in *17th International Conference on Microelectronics*, 2005, pp. 144 - 147.

[91] Swanson M and Guttman B, "Generally Accepted Principles and Practices for Securing Information Technology Systems", National Institute of Standards and Technology, Technology Administration 1996. Retrieved January 20, 2012 (csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf)

[92] Stallings W, *Cryptography and Netwrk Security*, 1st ed., Tracy Dunkelberger, Ed. New Jersey, United States of America: Pearson Prentice Hall, 2006.

[93] Kotzanikolaou P and Douligeris C, "Cryptography Primer: Introduction to Cryptographic Principles and Algorithms", in *Network Security: Current Status and Future Directions (IEEE Press)*, 2007, pp. 459 - 479.

[94] Zhang X, Heys H.M, and Li C, "Energy Cost of Cryptographic Session Key Establishment in a Wireless Sensor Network", in *International ICST Conference on Communications and Networking*, 2011, China, pp. 335 - 339.

[95] Weber S.G, "Harnessing Pseudonyms with Implicit Attributes for Privacy-Respecting Mission Log Analysis", in *International Conference on Intelligent Networking and Collaborative Systems*, 2009, pp. 119-126.

[96] Chaum D and Van Heyst E, "Group Signatures", in *Advances in Cryptography - EUROCRYPT*, 1991, Berlin, pp. 257-265.

[97] Boneh D, Boyen X, and Shacham H, "Short Group Signatures", in *CRYPTO - Advances in Cryptology*, Lecture Notes in Computer Science, 2004, vol. 3152, pp. 41 - 55.

[98] Calandriello G, Papadimitratos P, Hubaux J.P, and Lioy A, "Efficient and Robust Pseudonymous Authentication in VANETs", in *International ACM Conference on Vehicular Ad Hoc Networks*, Quebec, 2007, pp. 19 - 27.

[99] Armknecht F, Festag A, Westhoff D, and Zeng K, "Cross-layer Privacy Enhancement and Non-repudiation in Vehicular Communication", in *Workshop on Mobile Ad-Hoc Networks (WMAN)*, 2007, Bern, pp. 1 -12.

[100] Hildmann T and Wilke T.J, "Pseudonymous Authentication and Authorization enhancing ubiquitous Identity Management", Information Security Solutions Europe, Berlin, 2005. Retrieved September 26, 2011 (http://www.user.tu-berlin.de/hildcatf/Documents/ISSE2005-slides.pdf).

[101] Dawoud D.S, Van der Merwe J, and Peplow R, "Ensuring Privacy in Vehicular Communication", in *International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*, 2009, pp. 610 - 614.

[102] Manshaei M.H, Le Boudec J, Hubaux J.P, and Freudiger J, "On the Age of Pseudonyms in Mobile Ad Hoc Networks", in *IEEE International Conference on Computer Communications,* 2010, pp. 1 -9.

[103] Eichler S, "Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks depending on Node Mobility", in *IEEE Intelligent Vehicles Symposium*, Istanbul, Turkey, 2007, pp. 541 - 546.

[104] Yoon J.W and Kim H, "A new collision-free pseudonym scheme in Mobile Ad Hoc Networks", in *International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, 2009, pp. 1 - 5.

[105] Soh B, Phan H, Sunnadkal R, "A Four-Stage Design Approach Towards Securing a Vehicular Ad Hoc Networks Architecture", in *IEEE International Symposium on Electronic Design, Test & Applications*, 2010 , pp. 177 - 182.

[106] Festag A, Dirk Westhoff, Ke Zeng Frederik Armknecht, "Cross-layer Privacy Enhancement and Non-repudiation in Vehicular Communication", in *Workshop on Mobile Ad-Hoc Networks (WMAN)*, Bern, 2007, pp. 1 -12.

[107] Liao J and Li J, "Effectively Changing Pseudonyms for Privacy Protection in VANETs", in *International Symposium on Pervasive Systems, Algorithms, and Networks*, 2009, pp. 648 - 652.

[108] Ma Z, Kargl F, and Weber M, "Pseudonym-On-Demand: A New Pseudonym Refill Strategy for Vehicular Communications", in *IEEE International Symposium on Wireless Vehicular Communications (WiVeC 2008)*, 2008, Calgary, pp. 1 - 5.

[109] Freudiger J, Shokri R, and Hubaux J.P, *On the Optimal Placement of Mix Zones*, Goldberg and M. Atallah, Eds. Heidelberg, Berlin : Springer-Verlag, 2009.

[110] Yap W.S, Heng S.H, and Goi B.M, "Cryptanalysis of Some Proxy Signature Schemes Without Certificates", in *International Workshop on Information Security Theory and Practises, WISTP*, 2007, Greece, pp. 115 - 125.

[111] Petri S, "An Introduction to Smart Cards", Retrieved December 10, 2011 (www.artofconfusion.org/smartcards/docs/intro.pdf).

[112] Bhatt D.V, "Analysing the behaviour for a Smart Card based model for secure communication with remote computers over the internet", University of Pretoria, Pretoria, Master of Engineering Dissertation, 2010.

[113] CardLogix Corporation, "Welcome to Smart Card Basics", 2010. Retrieved December 12, 2011 (www.smartcardbasics.com/)

[114] Paradina P, Cordry J, and Bouzefrane S, "Performance Evaluation of Java Card Bytecodes", in *Workshop on Information Security Theory and Practices*, 2007, Greece, pp. 128 - 137.

[115] Itoi N, Fukuzawa T, and Honeyman P, "Secure Internet Smartcards", University of Michigan, Berlin, 2001. Retrieved February 18, 2012 (peter.honeyman.org/papers/secintsc.pdf).

[116] ChunXiao F, Junwei Z, Zhou P, and Xue Y, "An improved Dynamic Identity Authentication Scheme based on PKI-SIM Card", in *IEEE International Conference on Wireless Communications, Networking and Mobile Computing,* 2009, Beijing, pp. 1 - 4.

[117] Li Q, Zou J, and Zhang X, "The E-Bank Digital Signature Solution Based on PKI-SIM Cards", in *Proceedings of Iinternational Conference on Communications Technology and Applications*, 2009, pp. 900 - 902.

[118] Czerniewicz L, "Mobiles in Africa – some stats", November 2011. Retrieved March 23, 2012 (http://lauraczerniewicz.co.za/category/general/)

[119] Kohlas R and Maurer U, "*Reasoning About Public-Key Certification: On Bindings Between Entities and Public Keys",* IEEE Journal on Selected Areas in Communications, April 2000, vol. 18, no. 4, pp. 551 - 560.

[120] Vodacom, "Integrated Annual Report", March 2012. Retrieved November 10, 2012 (http://www.vodacom.com/inv_fin_ar.php).

[121] Selimis G, Fournaris A, Kostopoulos G, and Koufopavlou O, "Software and Hardware Issues in Smart Card Technology", *IEEE Communications Surveys and Tutorials*, 2009, vol. 11, no. 3, pp. 143 - 152.

[122] Bamberger O, Welter O, and Spitz S, "Mobile Phones as Secure Gateways for Message-Based Ubiquitous Communication", Technische University, Germany, IFIP International Federation for Information Processing 2007.

[123] Datamonitor, "United States - Smart Cards," United States of America, Industry Profile 72-379, 2001. Retrieved November 8, 2011 (http://connection.ebscohost.com/c/industry-overviews/11514409/united-states-smart-cards).

7. Bibliography

[1] Chandee M.S, Kumar D and Sheikh M.R, "Security Issues in MANET: A Review", *IEEE International Conference on Wireless And Optical Communications Networks,* September 2010, pp. 1 - 4.

[2] Biswas S and Misic J, "Deploying Proxy Signature In VANETs", in *IEEE Globecom 2010 proceedings*, 2010, pp. 1 - 6.

[3] Biswas S and Misic J, "Establishing Trust on VANET Safety Messages", University of Manitoba, Winnipeg, 2010.

[4] Biswas S and Misic J, "Proxy Signature-based RSU Message Broadcasting inVANETs", in *Biennial Symposium on Communications*, 2010, pp. 5 - 9.

[5] Stamp M and Low R.M, *Applied Cryptanalysis: Breaking Ciphers in the Real World*, 1st ed. Hoboken, New Jersey: John Wiley and Sons, 2007.

[6] Gollmann D, *Computer Security*, 2nd ed. Glasgov, Great Britain: John Wiley and Sons, 2006.

[7] Young A.L and Yung M, *Malicious Cryptography: Exposing Cryptovirology*, 1st ed. Indianapolis, Indiana: Wiley Publishing, 2004.

[8] Atallah E and Chaumette S, "A Smart Card Based Distributed Identity Management Infrastructure for Mobile Ad Hoc Networks", in *International Workshop on Information Security Theory and Principles, WISTP*, Greece, 2007, pp. 1 - 13.

[9] Rossudowski A.M and Venter H.S, "Secure Remote User Authentication over an Unsecure Telecommunications Network", University of Pretoria, Pretoria, Information and Computer Security Architectures (ICSA) Research Group Department of Computer Science.

[10] Jansen W, Gavrila S, and Séveillac C, "Smart Card Authentication for Mobile Devices", Edith Cowan University, School of Computer and Information Science, 2005.

[11] Millier B, BasicCards 101 (Part 1): Program your first Smart Card, 2001, Circuit Cellar; Magazine for Computer Applications. Retrieved January 24, 2012 (www.basiccard.com/circuit_cellar.pdf)

[12] Gao Z, Li Z, and Tu Y, "Design and completion of digital certificate with authorization based on PKI", in *Proceedings of the IEEE International Conference on Information Reuse and Integration*, 2004, pp. 462 - 466.

[13] Dempsey T, Sahin G, Morton Y.T, and Hopper C.M, "Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study", in *IEEE A&E Systems Magazine*, August 2009.

[14] Kafsi M, Papadimitratos P, Dousse O, Alpcan O, and Hubaux J.P, "VANET Connectivity Analysis", Nokia Research Center, Lausanne, 2009.

[15] Leavitt N, "Internet Security under Attack: The Undermining of Digital Certificates", *IEEE Computer Society Magazine: Technology News*, December 2011, vol. 44, no. 12, pp. 17 - 20.

[16] Many, *Vehicular Networking: Automotive Applications and Bayond*, 1st ed., M Emmelmann, B Bochow, and Kellum C C, Eds. Wiltshire, Great Britain: John Wiley and Sons, 2010.

[17] Lu R, Lin X, and Luan T.H, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs", *IEEE Transactions on Vehicular Technology*, July 2011, pp. 86 – 96.

[18] Boneh D, Sahai A, and Waters B, "Functional Encryption: Definitions and Challenges", in *Proceeedings of Conference on the Theory of Cryptography*, 2011,

Berlin, 253 - 273.

[19] Shi E, Bai F, Perrig A, and Studer A, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs", Carnegie Mellon University, CMU-CyLab Paper 24, 2008.

[20] Anjum F and Mouchtaris P, *Security for Wireless Ad Hoc Networks*, 1st ed. Hoboken, New Jersey: John Wiley and Sons, 2007.